# Vigor2110 系列
# 寬頻防火牆路由器
# 使用手冊

**UBLink 集團**

www.ublink.org

裕笠科技股份有限公司

遠豐科技股份有限公司

鉅創科技股份有限公司

# 目錄

## 1



## 2



## 3

4

# 1 前言

Vigor2110 series is a broadband router. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DS, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to **2 VPN tunnels**.

The object-based design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. CSM (Content Security Management) provides users control and management in IM (Instant Messenger) and P2P (Peer to Peer) more efficiency than before. By the way, DoS/DDoS prevention and URL/Web content filter strengthen the security outside and control inside.

Object-based firewall is flexible and allows your network be safe. In addition, through VoIP function, the communication fee for you and remote people can be reduced.

此外，Vigor2110 系列支援 USB 介面，可供連接 USB 印表機分享列印或是 USB 儲存裝置分享檔案，Vigor2110 系列提供二層式管理簡化網路連線設定，使用者模式讓使用者透過簡易設定達到存取網頁的目的，若是使用者想設定進階功能，可以透過管理者模式來處理。

## 1.1 網頁設定按鈕說明

在路由器的網頁設定中，有數種常見的按鈕，其定義如下所示：

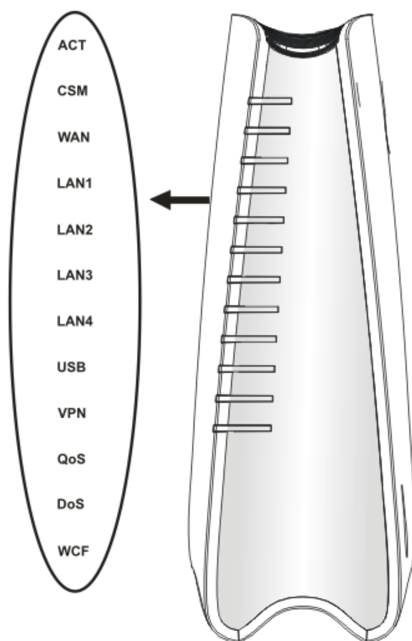
| 按鈕 | 說明 |
|---|---|
| 確定 | 儲存並套用目前的設定。 |
| 取消 | 取消目前設定並回復先前的設定值。 |
| 清除 | 捨棄目前設定值並允許使用者重新輸入。 |
| 新增 | 指定項目新增設定。 |
| 編輯 | 編輯選定項目的設定。 |
| 刪除 | 刪除選定項目及相關設定。 |

**附註:**有關網頁上所出現的其他按鈕，請參考第三、四章。

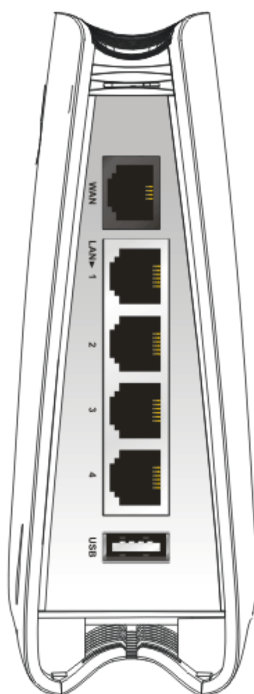
# 1.2 LED 指示燈與介面說明

不同機種路由器之 LED 顯示面板以及背板連接介面有些許的差異，詳列如下：

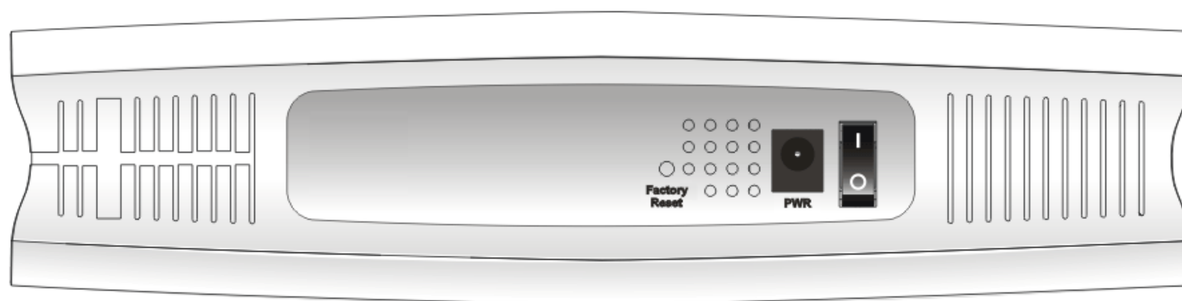
## 1.2.1 Vigor2110




| LED | Status | Explanation |
|---|---|---|
| LED 燈號 | 狀態 | 說明 |
| ACT (Activity) | 閃爍 | 路由器已開機並可正常運作。 |
| | 熄燈 | 路由器已關機。 |
| CSM<br>WAN | 亮燈 | 有關 IM/P2P, URL/Web Content Filter 應用等 CSM (Content Security Management) 設定檔，您可自**防火牆>>基本設定**中啓動使用. (啓動之前，必須先在 CSM 功能中建立好設定檔案。) |
| | 亮燈 | WAN 介面網路已連接。 |
| LAN 1/2/3/4 | 閃爍 | 正在傳輸資料中。 |
| | 亮燈 | 乙太網路已連接。 |
| | 熄燈 | 乙太網路未連接。 |
| USB | 閃爍 | 正在傳輸資料中。 |
| | 亮燈 | USB 裝置已連接並運作中。 |
| | 閃爍 | 正在傳輸資料中。 |
| VPN | 亮燈 | 虛擬私人網路功能已啓動。 |
| QoS | 亮燈 | QoS 功能已啓動。 |
| DoS | 亮燈 | DoS/DDoS 功能已啓動。 |
| | 閃爍 | 檢測到正受到外部攻擊。 |

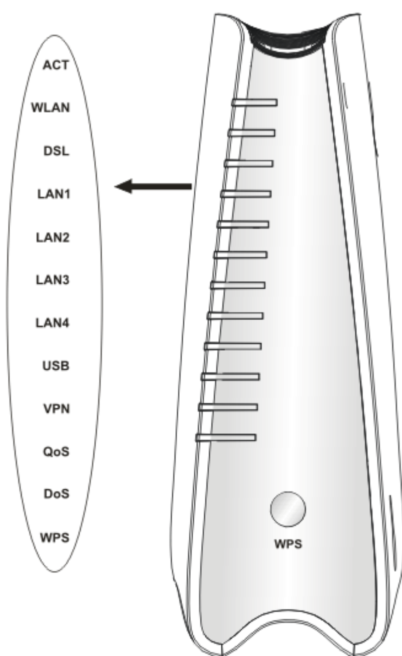



| 介面 | 說明 |
|---|---|
| WAN | 連接到 ADSL 或是 Cable Modem 裝置 |
| LAN (1-4) | 連接到電腦或網路設備 |
| USB | 連接到 USB 儲存裝置 (Pen Driver/Mobile HD) 或是印表機 |

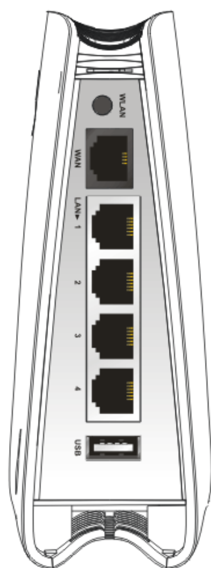



| 介面 | 說明 |
|---|---|
| Factory Reset | 還原成出廠預設值<br>用法：當路由器正在運作時（ACT LED 燈號閃爍），利用尖銳的物品（例如：原子筆）壓住 Factory Reset 超過 5 秒；當 ACT LED 燈號開始迅速閃爍時，鬆開此動作，路由器將會還原成出廠預設值 |
| PWR | 連接電源變壓器 |
| ON/OFF | 電源開關 |

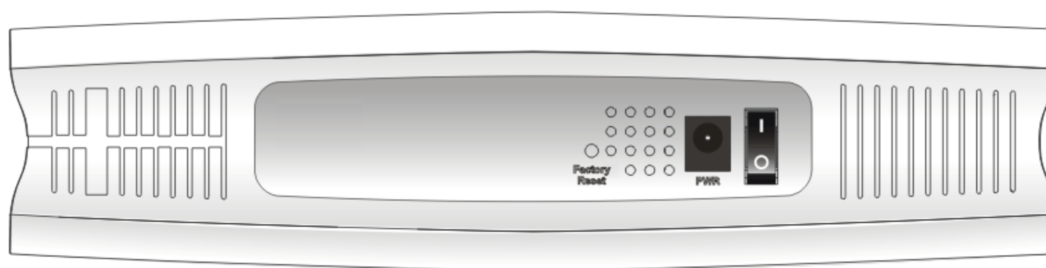
## 1.2.2 Vigor2110n




| LED 燈號 | 狀態 | 說明 |
|---|---|---|
| ACT (Activity) | 閃爍 | 路由器已開機並可正常運作。 |
| | 熄燈 | 路由器已關機。 |
| WLAN | 亮燈 | 無線 AP 預備妥當可以使用。 |
| | 閃爍 | 資料封包透過無線網路傳輸中。 |
| WAN | 亮燈 | WAN 介面網路已連接。 |
| | 閃爍 | 正在傳輸資料中。 |
| LAN 1/2/3/4 | 亮燈 | 乙太網路已連接。 |
| | 熄燈 | 乙太網路未連接。 |
| | 閃爍 | 正在傳輸資料中。 |
| USB | 亮燈 | USB 裝置已連接並運作中。 |
| | 閃爍 | 正在傳輸資料中。 |
| VPN | 亮燈 | 虛擬私人網路功能已啓動。 |
| QoS | 亮燈 | QoS 功能已啓動。 |
| DoS | 亮燈 | DoS/DDoS 功能已啓動。 |
| | 閃爍 | 檢測到正受到外部攻擊。 |
| WPS | 亮燈 | WPS 功能開啓。 |
| | 熄燈 | WPS 功能關閉。 |
| | 閃爍 | 等待無線用戶端傳送連線需求，約等 2 分鐘 |
| WPS 按鈕 | 亮燈 | 按住此鈕 2 分鐘等待用戶裝置透過 WPS 執行網路連線，當燈號亮起時，即表示 WPS 連線成功。 |
| | 熄燈 | WPS 功能關閉。 |
| | 閃爍 | 等待無線用戶端傳送連線需求，約等 2 分鐘。 |

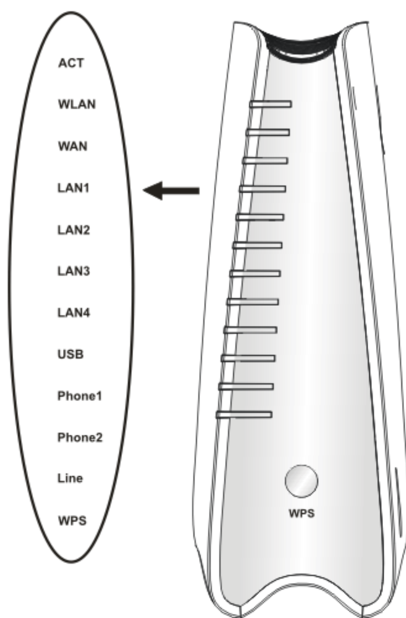


| 介面 | 說明 |
|---|---|
| WLAN | 按此鈕一次啓動(WLAN 燈號開啓)或是關閉(WLAN 燈號關閉啓)無線連線。 |
| WAN | 連接到 ADSL 或是 Cable Modem 裝置。 |
| LAN (1-4) | 連接到電腦或網路設備。 |
| USB | 連接到 USB 儲存裝置（Pen Driver/Mobile HD）或是印表機。 |

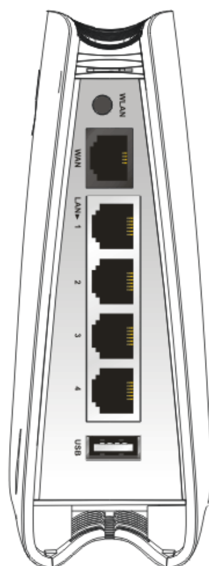



| 介面 | 說明 |
| --- | --- |
| Factory Reset | 還原成出廠預設值<br>用法：當路由器正在運作時（ACT LED 燈號閃爍），利用尖銳的物品（例如：原子筆）壓住 Factory Reset 超過 5 秒；當 ACT LED 燈號開始迅速閃爍時，鬆開此動作，路由器將會還原成出廠預設值 |
| PWR | 連接電源變壓器 |
| ON/OFF | 電源開關 |

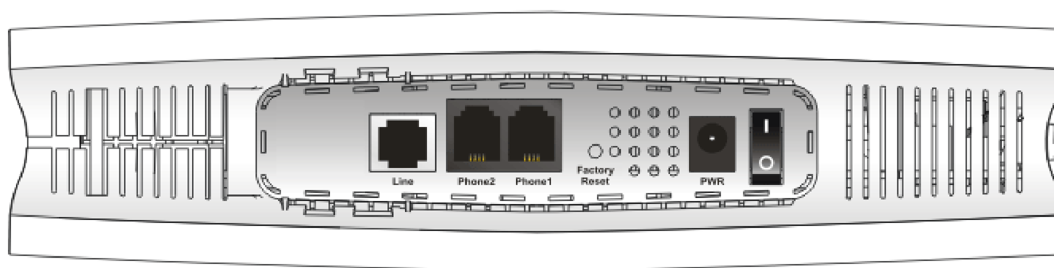
### 1.2.3 Vigor2110Vn




| LED 燈號 | 狀態 | 說明 |
|---|---|---|
| ACT (Activity) | 閃爍 | 路由器已開機並可正常運作。 |
| | 熄燈 | 路由器已關機。 |
| WLAN | 亮燈 | 無線 AP 預備妥當可以使用。 |
| | 閃爍 | 資料封包透過無線網路傳輸中。 |
| WAN | 亮燈 | WAN 介面網路已連接。 |
| | 閃爍 | 正在傳輸資料中。 |
| LAN 1/2/3/4 | 亮燈 | 乙太網路已連接。 |
| | 熄燈 | 乙太網路未連接。 |
| | 閃爍 | 正在傳輸資料中。 |
| USB | 亮燈 | USB 裝置已連接並運作中。 |
| | 閃爍 | 正在傳輸資料中。 |
| Phone1/ Phone2 | 亮燈 | 連接本埠之電話使用中。 |
| | 熄燈 | 連接本埠之電話未被使用。 |
| | 閃爍 | 電話來電。 |
| Line | 亮燈 | PSTN 電話撥進或撥出，不過當電話斷線時，LED 燈號約需六秒鐘才會熄滅。 |
| | 熄燈 | 目前沒有 PSTN 電話。 |
| WPS | 亮燈 | WPS 功能開啓。 |
| | 熄燈 | WPS 功能關閉。 |
| | 閃爍 | 等待無線用戶端傳送連線需求，約等 2 分鐘 |
| WPS 按鈕 | 亮燈 | 按住此鈕 2 分鐘等待用戶裝置透過 WPS 執行網路連線，當燈號亮起時，即表示 WPS 連線成功。 |
| | 熄燈 | WPS 功能關閉。 |
| | 閃爍 | 等待無線用戶端傳送連線需求，約等 2 分鐘。 |



| 介面 | 說明 |
|---|---|
| WLAN | 按此鈕一次啓動(WLAN 燈號開啓)或是關閉(WLAN 燈號關閉啓)無線連線。 |
| WAN | 連接到 ADSL 或是 Cable Modem 裝置。 |
| LAN (1-4) | 連接到電腦或網路設備。 |
| USB | 連接到 USB 儲存裝置（Pen Driver/Mobile HD）或是印表機。 |

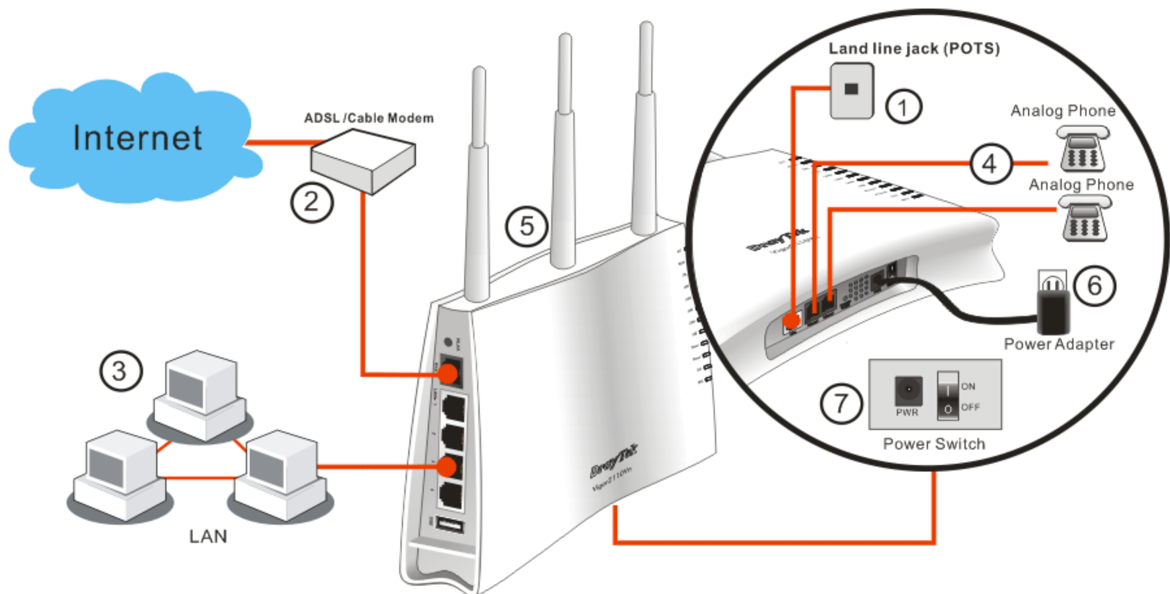



| Interface | Description |
|---|---|
| Line | 連接 PSTN life 線 |
| Phone2/Phone1 | 連接類比電話機，以便使用 VoIP 通話功能 |
| Factory Reset | 還原成出廠預設值<br>用法：當路由器正在運作時（ACT LED 燈號閃爍），利用尖銳的物品（例如：原子筆）壓住 Factory Reset 超過 5 秒；當 ACT LED 燈號開始迅速閃爍時，鬆開此動作，路由器將會還原成出廠預設值 |
| PWR | 連接電源變壓器 |
| ON/OFF | 電源開關 |

## 1.3 硬體安裝

設定路由器前，請先將裝置確實連接，並參考以下步驟操作。

1. 利用網路纜線(RJ-11) 連接此裝置至牆壁的電話插座上 (Vn 機型)。
2. 利用乙太網路纜線(RJ-45)將數據機/路由器連接到本裝置的 WAN 連接埠。
3. 利用乙太網路纜線(RJ-45)一端連接 PC 的乙太網路連接埠，一端連接到路由器任何一個 **LAN** 連接埠。
4. 將類比電話機安裝至 Phone 連接埠。
5. 安裝天線 (n 機型)。
6. 將電源線一端連接到路由器，另一端連接到牆上電源輸出孔。
7. 開啓路由器。
8. 檢查 **ACT** 及 **WAN, LAN** 燈號是否亮燈，以確定硬體連線有否成功。

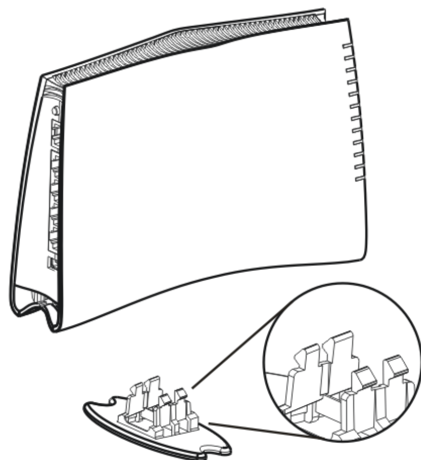



**注意:**
1. 每個電話埠都僅能連接類比話機，請勿直接將 Phone 連接埠與牆壁的電話插座相連，以免造成路由器毀損。
2.當電源中斷時，VoIP 電話也會被中斷，但是連接至 Phone 2 埠之話機可以如傳統話機一般的使用，這是因為該線已被路由器導引至牆壁的電話插座線路上(電話介接)。

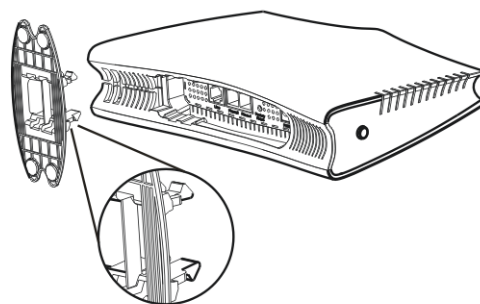
## 腳座安裝

Vigor2110 必須直立放置以確保正常操作，因此您需要爲其安裝一個腳座，使其能夠穩當站立。請依照下列圖示來完成正確的安裝：

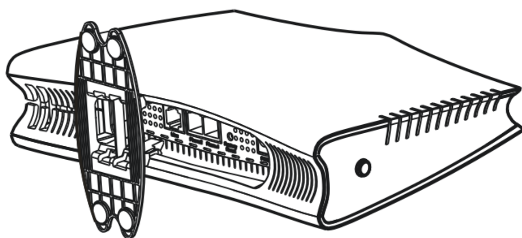
①



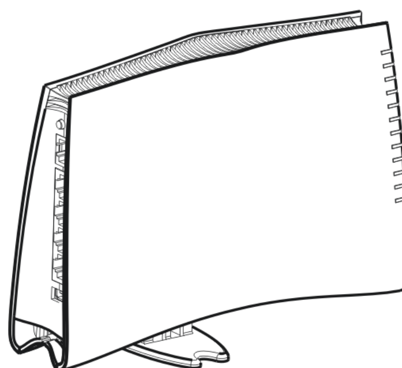
②



③

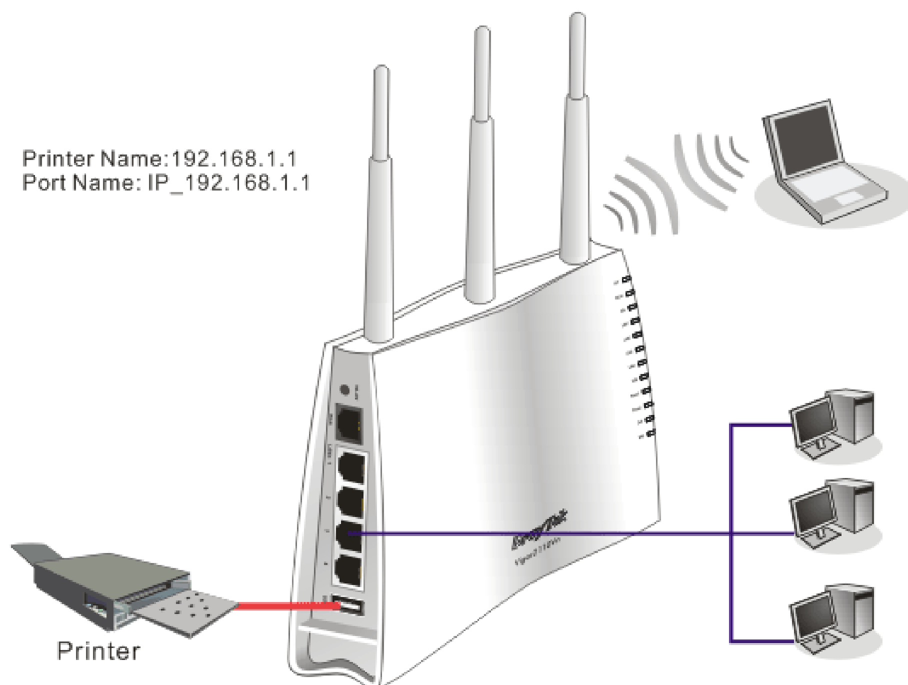


④



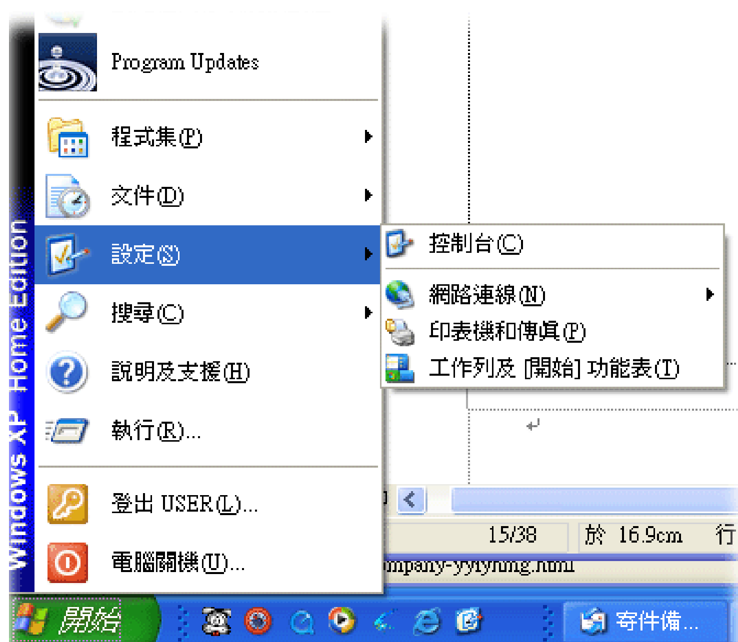
## 1.4 印表機安裝

您可以在路由器上連接印表機來分享列印功能，這樣路由器的區域網路上所有的電腦都可透過它列印文件，以下設定範例是以 Windows XP/2000 為主，如果您使用的是 Windows 98/SE/Vista，請造訪居易網站 www.draytek.com 取得您所需要的安裝資訊。




使用之前，請務必按照下列步驟來設定您的電腦（或無線用戶）：

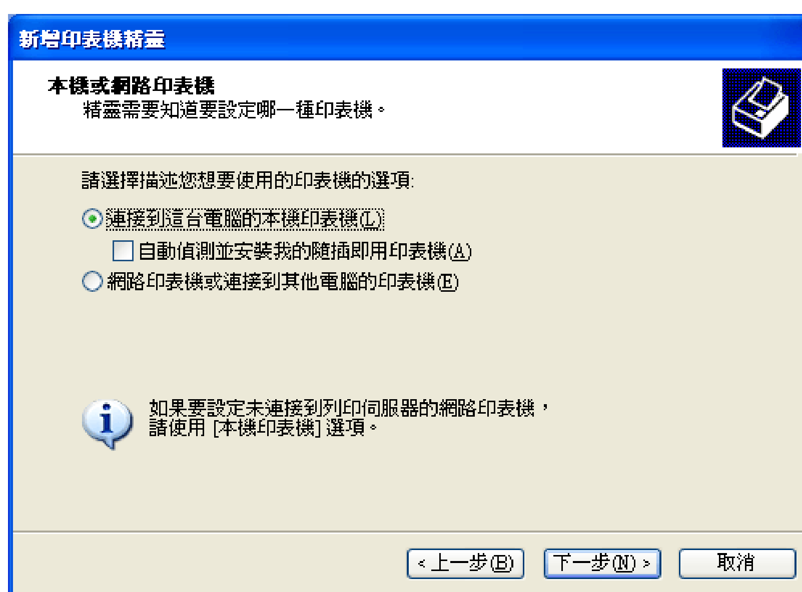
1. 請透過 USB 連接埠連接印表機與路由器。
2. 開啟**開始>>設定>>印表機和傳真**。



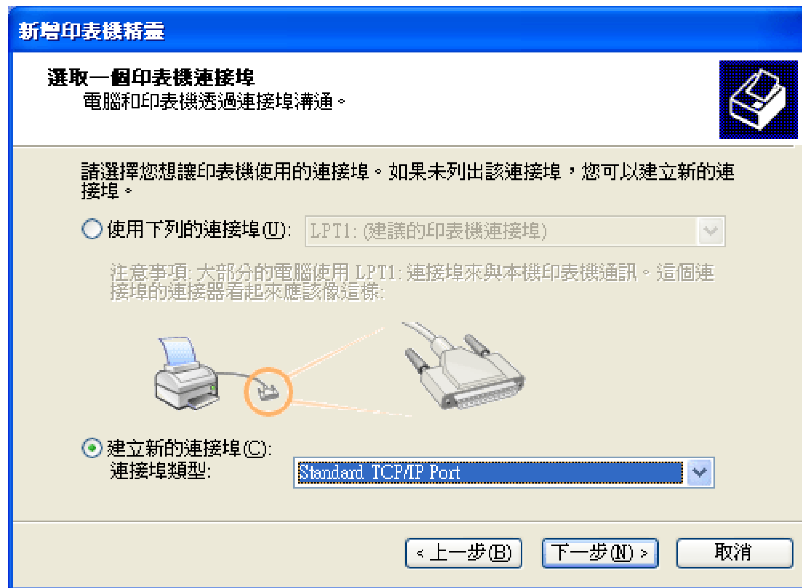

3. 開啟**檔案>>新增印表機**，設定精靈將會出現，請按**下一步**。




4. 選擇"**連接到這台….**"並按**下一步**。



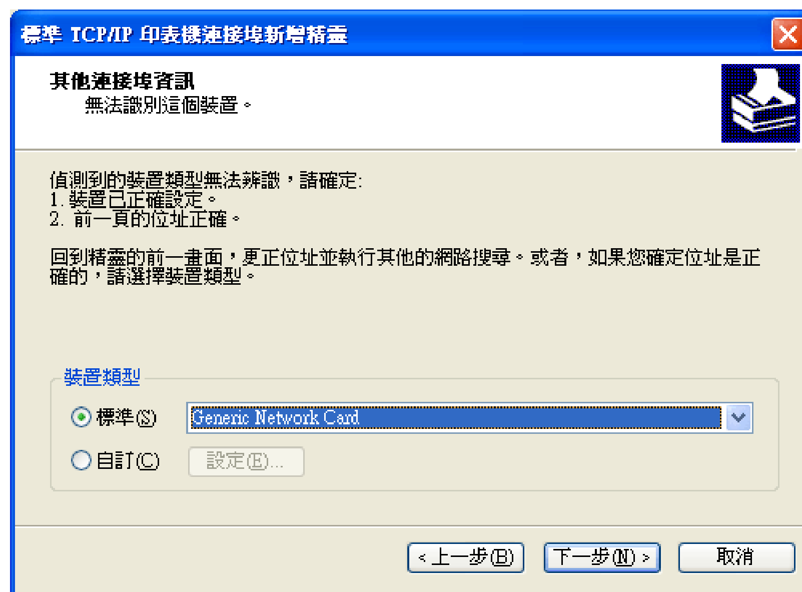
5. 接著請選擇 “**建立新的連接埠**”，用下拉式選項選擇“**Standard TCP/IP Port**”， 按**下一步**。




6. 在下面的對話方塊中，請輸入 **192.168.1.1** (路由器的 LAN IP)，**IP_192.168.1.1** 會自動帶出，再按**下一步**。



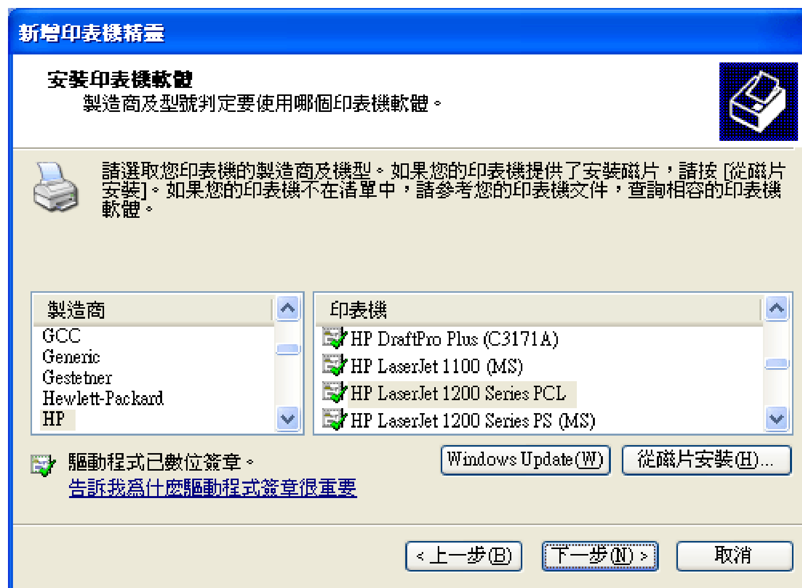
7. 請選擇**標準**，並自下拉式選項中選取 **Generic Network Card**。



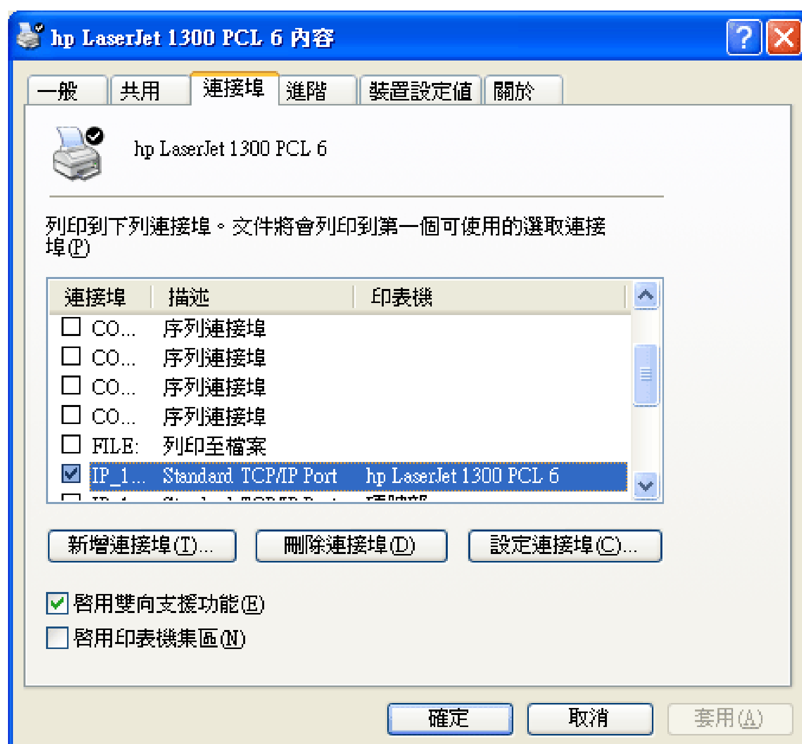

8. 當下列畫面出現時，請按**完成**。



9. 現在系統將會要求您選擇您安裝至路由器上的印表機名稱，這個步驟可以讓您的電腦安裝正確的驅動程式，當您完成項目選擇之後，請按**下一步**。




10. 最後請您回到**印表機和傳真**頁面，編輯您新增印表機的內容。



11. 在通訊協定欄位中，選擇"**LPR**"，佇列名稱則請輸入”p1”，按下**確定**鈕。

設定標準 TCP/IP 連接埠監視器

連接埠設定值

連接埠名稱(P): IP_172.16.3.227

印表機名稱或 IP 位址(A): 172.16.3.227

通訊協定

Raw(R) LPR(L)

Raw 設定

連接埠號碼(N): 515

LPR 設定

佇列名稱(Q): p1

啟用 LPR 位元組計數(B)

啟用 SNMP 狀態(S)

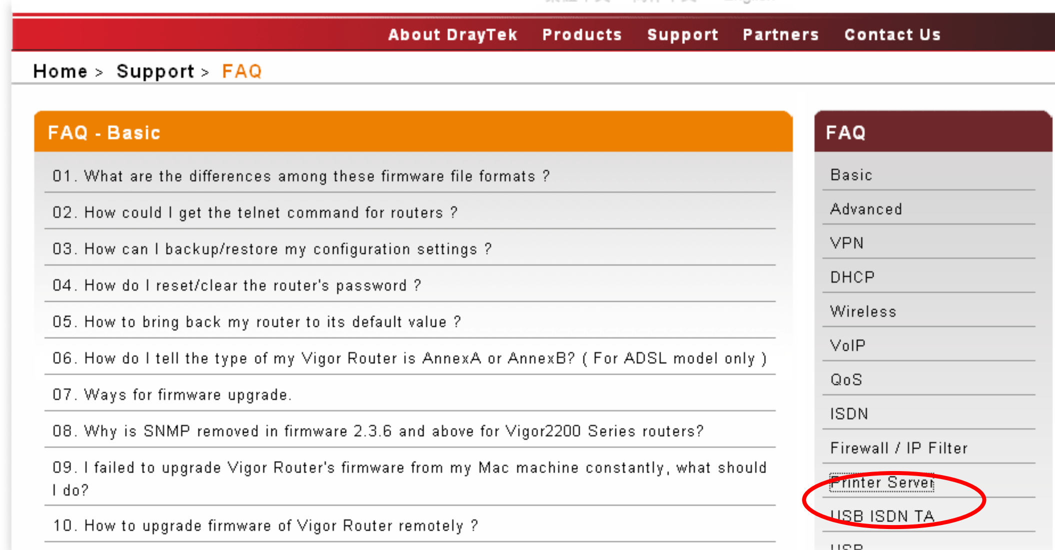
群體名稱(C): public

SNMP 裝置索引(D): 1

確定 取消

您現在可以使用新增的印表機了，大多數的印表機都與 Vigor 路由器相容。

**注意 1:** 此路由器仍不支援市面上某些印表機，如果您不知道自己所購買的印表機有無在支援之列，請造訪 www.draytek.com，上面可輕易取得您想知道的訊息，開啓 **Support Center->FAQ**; 按下 **Printer Server** 連結，接著再按下 **What types of printers are compatible with Vigor router?** 連結，即可獲得您要的內容。



FAQ - Printer Server

01. How do I configure LPR printing on Windows2000/XP ?
02. How do I configure LPR printing on Windows98/Me ?
03. How do I configure LPR printing on Linux boxes ?
04. Why there are some strange print-out when I try to print my documents through Vigor2104P / 2300's print server?
05. What types of printers are compatible with Vigor router?
06. What are the limitations in the USB Printer Port of Vigor Router ?
07. What is the printing buffer size of Vigor Router ?
08. How do I configure LPR printing on Mac OSX ?
09. How do I configure LPR printing on My Windows Vista ?

**注意 2:** Vigor 路由器支援來自 LAN 端的列印要求，但不支援來自 WAN 端的列印要求。

# 2 基本設定

在開始使用路由器時，基於安全的考量，我們強烈建議你在路由器上設定一組管理者密碼。

## 2.1 二層管理

This chapter explains how to setup a password for an administrator/user and how to adjust basic/advanced settings for accessing Internet successfully.

For user mode operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for admin mode operation, please type “admin/admin” on Username/Password and click **Login** for full configuration.

## 2.2 進入網頁

1. 確保您的電腦已經和路由器正確的連接。



> 附註: 您可以選擇直接設定電腦的網路設定爲動態取得 IP 位址 (DHCP)，或者是將 IP 設定爲和 IP 分享器的預設 IP 位址 (192.168.1.1) 於同一個子網路。如需更多訊息，請參考後面的章節 – 疑難排解。

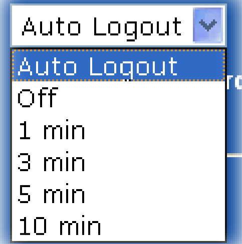
2. 開啓網頁瀏覽器並輸入位址 http://192.168.1.1，登入視窗將會出現。

3. For user mode operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for admin mode operation, please type “admin/admin” on Username/Password and click **Login** for full configuration.



> **Notice:** If you fail to access to the web configuration, please go to “Trouble Shooting” for detecting and solving your problem.

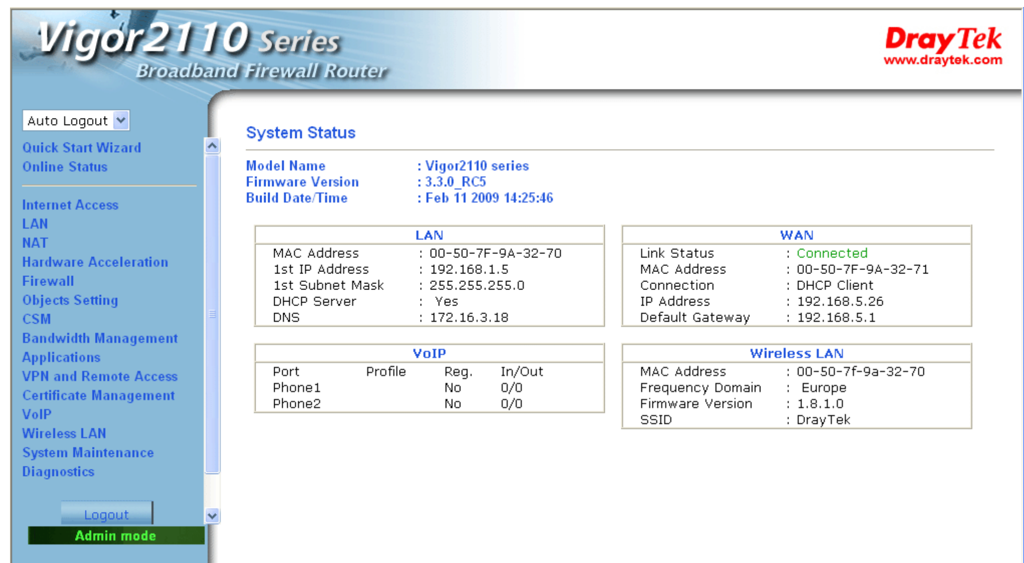
4. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



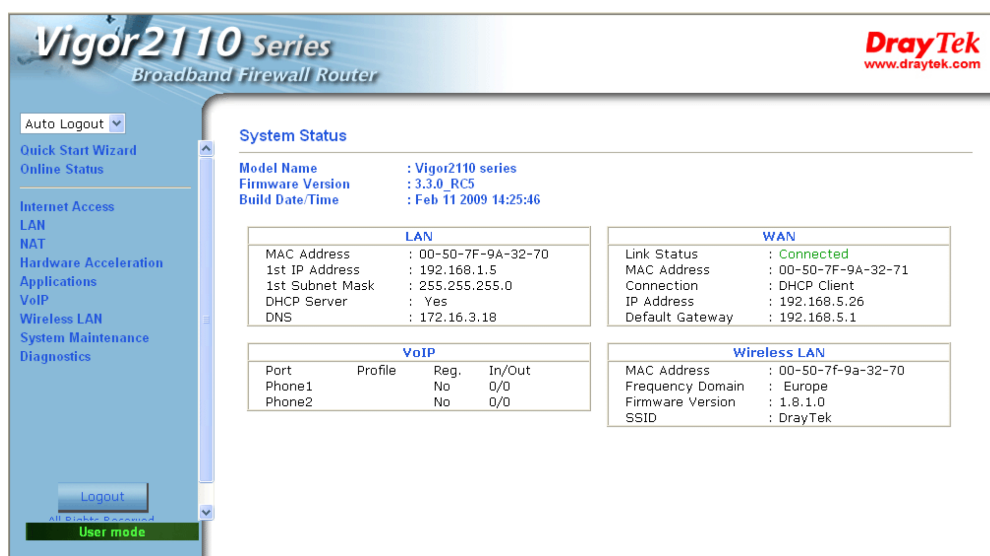

## 2.3 變更密碼

無論是使用者操作模式或是管理者操作模式，建議您將密碼先行變更。

1. 開啓網頁瀏覽器並輸入位址 http://192.168.1.1。登入視窗將會出現並要求您輸入使用者名稱與密碼。
2. 請輸入 “admin/admin”進入管理者模式，或將欄位空白什麼都不要輸入，以進入使用者模式，然後按下**登入**進入網頁。
3. 現在，設定介面的主選單會出現。




**管理者操作模式主畫面（完整設定）**




**使用者操作模式主畫面 (簡易設定)**

注意： 因為首頁會依照您的路由器的功能做些微改變，所以設定介面不一定都會如上圖所示。

4. 進入**系統維護**頁面並選擇**系統管理員/使用者密碼**。

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password

New Password

Confirm Password

OK

*或是*

System Maintenance >> User Password

User Password

Old Password

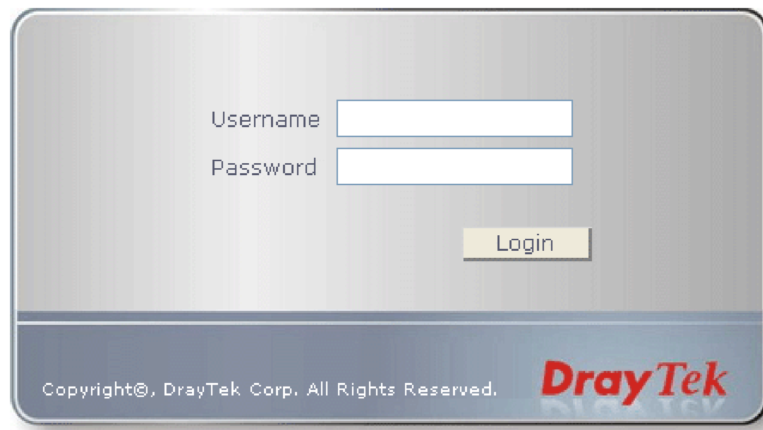
New Password

Confirm Password

OK

5. 輸入舊密碼 (預設值為空白)。 在**新密碼**及**確認密碼**輸入您想要設定的密碼，然後按**確定**儲存設定。

6. 現在您已經完成變更密碼設定。請記得在下一次登入設定介面時使用新的密碼。




## 2.4 快速設定精靈



**注意**:快速安裝精靈在使用者模式中的操作與管理者模式下操作是相同的。

如果您打算佈建此路由器在現成的高速 NAT 網路結構中，您可以依照下列的步驟使用快速設定精靈設定您的路由器。快速設定精靈的第一個畫面會要求您輸入密碼，輸入密碼之後，請按**下一步**。

**Quick Start Wizard**

**Enter login password**

Please enter an alpha-numeric string as your **Password** (Max 23 characters).

Old Password

New Password

Confirm Password

< Back | Next > | Finish | Cancel

在下圖顯示中，請依照您的 ISP 提供的資料，選擇適當的網際網路連線類型，例如 ISP 提供您 PPPoE 介面的資訊，您就應該選擇 PPPoE 模式。接著按**下一步**進行。

Quick Start Wizard

Connect to Internet

WAN 1

Select one of the following Internet Access types provided by your ISP.

- (•) PPPoE
- ( ) PPTP
- ( ) Static IP
- ( ) DHCP

< Back | Next > | Finish | Cancel

## 2.4.2 PPPoE

PPPoE 為 Point-to-Point Protocol over Ethernet 的縮寫，是一種利用個人電腦透過寬頻連接設備(如 xDSL、Cable、Wireless)連接至高速寬頻網路的技術，用戶僅需在個人的電腦上加裝乙太網路卡，然後向電信線路提供者(如：中華電信)與網際網路服務提供者(ISP，如：亞太線上)申請 ADSL 服務，就可以以類似傳統撥接的方式，透過一般的電話線連上網際網路。另外，PPPoE 也同時被用來在 ADSL 網路架構上進行用戶認證、紀錄用戶連線時間，以及取得動態 IP。

如果您的 ISP 業者提供您 PPPoE 連線方式， 請先在視窗中選擇適當的模式，然後輸入相關資訊：

Quick Start Wizard

PPPoE Client Mode

WAN 1

Enter the user name and password provided by your ISP.

| | |
|---|---|
| User Name | 123 |
| Password | ●●● |
| Confirm Password | ●●● |

< Back | Next > | Finish | Cancel

**使用者名稱** 指定 ISP 提供之有效使用者名稱。

**密碼** 指定 ISP 提供之有效密碼。

**確認密碼** 重新輸入密碼以確認。

按**下一步**檢視此連線的設定狀態。

Quick Start Wizard

Please confirm your settings:

| | |
|---|---|
| WAN Interface: | WAN1 |
| Physical Mode: | Ethernet |
| Physical Type: | Auto negotiation |
| Internet Access: | PPPoE |

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

< Back Next > Finish Cancel

按**完成**，快速入門設定精靈安裝完畢將會出現，接著此協定的系統狀態將會顯示於後。

### 2.4.3 PPTP

PPTP 則是 Point-to-Point Tunneling Protocol 的簡稱。有些 DSL 服務提供者採用一種特別的 DSL 數據機(例如：阿爾卡特的 DSL 數據機)。這種數據機只支援 PPTP Tunnel 方法存取 Internet。在這種情形下，您建立一個到 DSL 數據機並且帶有 PPP Session 的 PPTP Tunnel。一但 Tunnel 建立後，這種 DSL 數據機會將 PPP Session 送往 ISP。當 PPP Session 建立後，當地的使用者共用這個 PPP Session 存取 Internet。如果您需要使用 PPPTP 連線，請先在視窗中選擇適當的模式，然後輸入相關資訊：

Quick Start Wizard

PPTP Client Mode

WAN 1

Enter the user name, password, WAN IP configuration and PPTP server IP provided by your ISP.

| | |
|---|---|
| User Name | 123 |
| Password | ••• |
| Confirm Password | ••• |
| WAN IP Configuration | |
| ◉ Obtain an IP address automatically | |
| ○ Specify an IP address | |
| IP Address | |
| Subnet Mask | |
| Gateway | undefined |
| Primary DNS | undefined |
| Second DNS | undefined |
| PPTP Server | |

< Back | Next > | Finish | Cancel

按**下一步**檢視此連線的設定狀態。

Quick Start Wizard

Please confirm your settings:

| | |
|---|---|
| WAN Interface: | WAN1 |
| Physical Mode: | Ethernet |
| Physical Type: | Auto negotiation |
| Internet Access: | PPTP |

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

< Back | Next > | Finish | Cancel

按**完成**，快速入門設定精靈安裝完畢將會出現，接著此協定的系統狀態將會顯示於後。

## 2.4.4 固定 IP

在這種應用當中，您會從 ISP 取得一個固定真實 IP 位址或一個真實子網路(多個公開 IP 位址)。通常纜線(Cable) ISP 會提供一個固定的真實 IP，而 DSL ISP 則有可能會提供一個真實子網路。如果您擁有一個真實子網路，您可以選擇一個或多個 IP 位址設定在 WAN 介面。如果您需要使用固定 IP / 動態 IP，請先在視窗中選擇適當的模式，然後輸入相

關資訊：

Quick Start Wizard

Static IP Client Mode

WAN 1

Enter the Static IP configuration probided by your ISP.

| | |
|---|---|
| WAN IP | 172.16.3.229 |
| Subnet Mask | 255.255.0.0 |
| Gateway | 172.16.3.4 |
| Primary DNS | |
| Secondary DNS | (optional) |

< Back | Next > | Finish | Cancel

設定輸入完畢之後，按**下一步**檢視此連線的設定狀態。

Quick Start Wizard

Please confirm your settings:

| | |
|---|---|
| WAN Interface: | WAN1 |
| Physical Mode: | Ethernet |
| Physical Type: | Auto negotiation |
| Internet Access: | Static IP |

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

< Back | Next > | Finish | Cancel

按**完成**，快速入門設定精靈安裝完畢將會出現，接著此協定的系統狀態將會顯示於後。

## 2.4.5 DHCP

選擇 **DHCP** 作爲通訊協定，並在頁面上輸入 ISP 提供給您的全部訊息。

Quick Start Wizard

DHCP Client Mode

WAN 1

If your ISP requires you to enter a specific host name or specific MAC address, please enter it in.

Host Name (optional)

MAC 00 - 50 - 7F - 92 - F5 - 61 (optional)

< Back Next > Finish Cancel

設定輸入完畢之後，按**下一步**檢視此連線的設定狀態。

Quick Start Wizard

Please confirm your settings:

| | |
|---|---|
| WAN Interface: | WAN1 |
| Physical Mode: | Ethernet |
| Physical Type: | Auto negotiation |
| Internet Access: | DHCP |

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

< Back Next > Finish Cancel

按**完成**，快速入門設定精靈安裝完畢將會出現，接著此協定的系統狀態將會顯示於後。

## 2.5 線上狀態

線上狀態顯示出系統目前執行的情形，WAN 連接狀況，ADSL 資訊和其他與路由器有關的訊息。如果您選擇 PPPoE 作爲通訊協定，您可發現頁面上出現一個 **Dial PPPoE** 或 **Drop PPPoE** 的按鈕。

**Online status for DHCP**

Online Status

| System Status | | | | | System Uptime: 4:7:24 |
|---|---|---|---|---|---|
| LAN Status | | Primary DNS: 172.16.3.18 | | Secondary DNS: 168.95.1.1 | |
| IP Address | TX Packets | RX Packets | | | |
| 192.168.1.5 | 21848 | 32232 | | | |
| WAN Status | | | | | >> Release |
| Enable | Line | Name | Mode | Up Time | |
| Yes | Ethernet | | DHCP Client | 4:07:16 | |
| IP | GW IP | TX Packets | TX Rate(Bps) | RX Packets | RX Rate(Bps) |
| 192.168.5.26 | 192.168.5.1 | 10538 | 11 | 10547 | 26 |

詳細說明於後：

| | |
|---|---|
| **主要 DNS** | 顯示主要 DNS 的 IP 位址。 |
| **次要 DNS** | 顯示次要 DNS 的 IP 位址。 |
| ***區域網路狀態*** | |
| **IP 位址** | 顯示區域網路介面的 IP 位址。 |
| **傳送封包** | 顯示在區域路中全部的傳送封包量。 |
| **接收封包** | 顯區域路中全部的接收封包量。 |
| ***WAN 狀態*** | |
| **實體模式** | 顯示實體介面連線的狀態。 |
| **顯示名稱** | 顯示 WAN1/WAN 網頁上所顯示的名稱。 |
| **模式** | 顯示 WAN 連接(PPPoE)的類型。 |
| **連線時間** | 顯示介面上全部的上傳時間。 |
| **閘道 IP** | 顯示預設閘道的 IP 位址。 |
| **傳送封包** | 顯示 WAN 介面上全部傳送的封包數。 |
| **傳送速率** | 顯示 WAN 介面上全部傳送速率位元數。 |
| **接收封包** | 顯示 WAN 介面上全部接收的封包數。 |
| **接收速率** | 顯示 WAN 介面上全部接收速率位元數。 |

**注意:**綠色字樣表示該 WAN 連接已預備妥當，隨時可以存取網際網路資料，紅色字樣則表示該 WAN 連接尚未預備妥當，也還無法透過路由器存取網際網路資料。

## 2.6 儲存設定

每當您按下網頁上的確定按鈕以儲存檔案，您都可以見到如下的訊息，此爲系統提供的狀態通知。

Status: Ready

**預備**表示系統處於預備狀態隨時可以輸入設定。

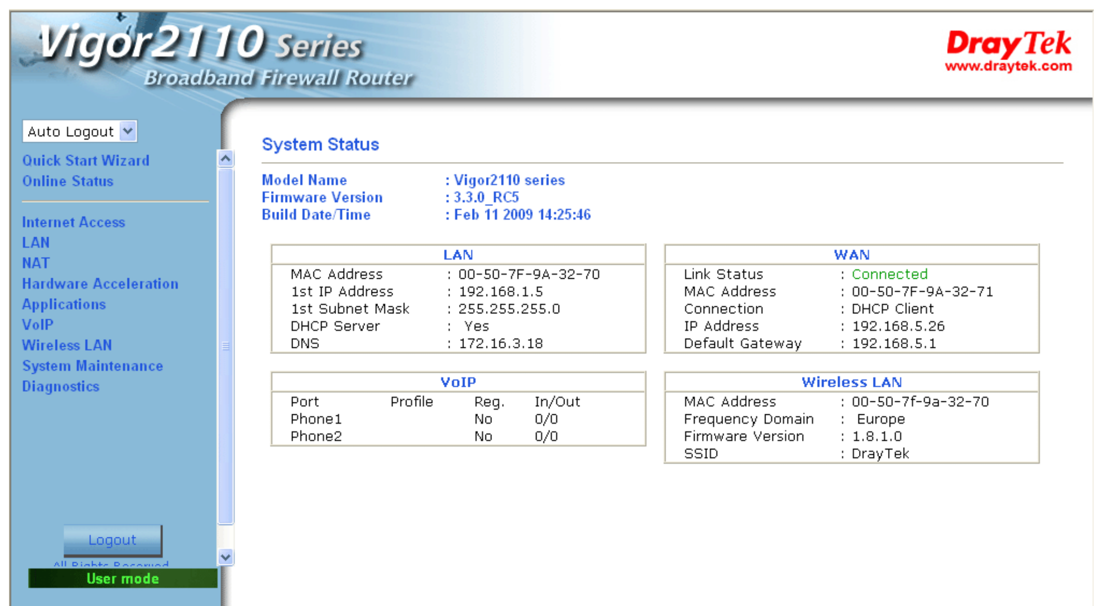
**設定已儲存**表示您按了完成或是確定按鈕之後，系統已儲存該設定。

# 3 使用者操作模式

This chapter will guide users to execute simple configuration through user mode operation. As for other examples of application, please refer to chapter 5.

1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.
2. **Do not** type any word (both username and password are Null for user operation) on the window and click **Login** on the window.

Now, the **Main Screen** will appear. Be aware that "User mode" will be displayed on the bottom left side.




## 3.1 Internet Access

快速安裝精靈提供使用者一個簡單的方法，以便能快速設定路由器的連線模式。如果您想要針對不同廣域網路模式調整更多的設定，請前往 **Internet Access** 群組然後點選**網際網路連線控制**連結。

### 3.1.1 IP 網路的基本概念

IP 表示網際網路通訊協定，在以 IP 為主的網路像是路由器、列印伺服器和主機電腦的每一種裝置，都需要一組 IP 位址作為網路上身分辨識之用。為了避免位址產生衝突，IP 位址都必須於網路資訊中心(NIC) 公開註冊，擁有個別 IP 位址對那些於真實網路分享的裝置是非常必要的，但在虛擬網路上像是路由器所掌管下的主機電腦就不是如此，因為它們不需要讓外人從真實地區進入存取資料。因此 NIC 保留一些永遠不被註冊的特定位址，這些被稱之為虛擬 IP 位址，範圍條列如下：

**從 10.0.0.0 到 10.255.255.255**
**從 172.16.0.0 到 172.31.255.255**
**從 192.168.0.0 到 192.168.255.255**

### 什麼是真實 IP 位址和虛擬 IP 位址

由於路由器扮演著管理及保護其區域網路的角色，因此它可讓主機群間互相聯繫。每台主機都有虛擬 IP 位址，是由路由器的 DHCP 伺服器所指派，路由器本身也會使用預設之虛擬 IP 位址 192.168.1.1 與本地主機達成聯繫目的，同時，Vigor 路由器可藉由真實 IP 位址與其他的網路裝置溝通連接。當資料經過時，路由器的網路位址轉換(NAT)功能將會在真實與虛擬位址間執行轉換動作，封包將可傳送至本地網路中正確的主機電腦上，如此一來，所有的主機電腦就都可以共享一個共同的網際網路連線。

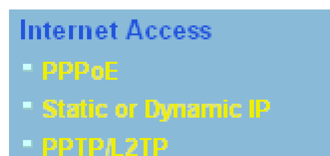
### 取得 ISP 提供的真實 IP 位址

欲取得 ISP 提供的真實 IP 位址，以便將路由器當成用戶假定之設備，有幾種種常見的模式可以選用：**Point to Point Protocol over Ethernet (PPPoE),** 和 **MPoA**.等，**Multi-PVC** 是提供給您執行更進階的設定。

在 ADSL 之部署中，PPP (Point to Point)型態之驗證和授權是橋接用戶前端設備所需要的。PPPoE (Point to Point Protocol over Ethernet )透過一台存取裝置連接網路主機至遠端存取集中器，此種應用讓使用者覺得操作路由器是很簡單的，同時也可依照使用者的需要提供存取控制及服務類型。

當路由器開始連接至 ISP 時，路由器將執行一系列過程以尋求連線，然後即可產生一個 session，您的使用者辨識名稱和密碼由 **RADIUS** 驗證系統的 **PAP** 或 **CHAP** 來驗證，通常您的 IP 位址、DNS 伺服器和其他相關資訊都是由 ISP 指派的。

下圖為 **Internet Access**.的功能項目：




## 3.1.2 PPPoE

如果想要使用 PPPoE 作為網際網路連線的通訊協定，請自 **Internet Access** 功能項目中選擇 **PPPoE** 模式，下面的設定網頁將會出現。

Internet Access >> PPPoE

PPPoE Client Mode

| PPPoE Setup | | PPP/MP Setup | |
|---|---|---|---|
| PPPoE Link | ○ Enable ⦿ Disable | PPP Authentication | PAP or CHAP |
| ISP Access Setup | | ☑ Always On | |
| Username | | Idle Timeout | -1 second(s) |
| Password | | IP Address Assignment Method (IPCP) | WAN IP Alias |
| Index(1-15) in Schedule Setup: | | Fixed IP | ○ Yes ⦿ No (Dynamic IP) |
| => , , , | | Fixed IP Address | |
| WAN Connection Detection | | ⦿ Default MAC Address | |
| Mode | ARP Detect | ○ Specify a MAC Address | |
| Ping IP | | MAC Address: | 00 .50 .7F :9A .32 .71 |
| TTL: | | | |

OK

**PPPoE 用戶端模式**

按下**啟用**按鈕可啟動此功能，如果您選的是**停用**，此項功能將會關閉，全部調整過的設定也都將立即失效。

**ISP 存取設定**

輸入使用者名稱、密碼和驗證參數，按照 ISP 所提供給您的訊息。

**使用者名稱** –在本區請輸入 ISP 提供的使用者名稱。

**密碼** – 在本區請輸入 ISP 提供的密碼。

**索引號碼(1-15) 於排程設定** -可以輸入四組時間排程，全部的排程都是在**應用-排程**網頁中事先設定完畢，您可在此輸入該排程的索引編號。

**WAN 連線檢測**

這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。

模式 – 選擇 **ARP Detect** **或** **Ping Detect** 執行 WAN 檢測動作。

**Ping IP** – 如果您選擇 **Ping Detect** 作爲檢測模式，您必須在本區輸入 IP 位址作爲 Ping 檢測之用。

**TTL (Time to Live)** – 顯示數値供您參考，TTL 數値是利用 Telnet 指令始可設定。

**PPP/MP 設定**

**PPP 驗證** – 選擇 **PAP** 或是 **PAP 或 CHAP**。

**閒置逾時** – 設定網際網路在經過一段沒有任何動作的時間後自動斷線的時間，此項設定只在 **WAN>>一般設定**網頁中的**啟動模式**選擇了**需求時連線**才會有作用。

**IP 位址指派方式 (IPCP)**

通常每次的連線，ISP 會隨機指派 IP 位址給您，在某些情況下，您的 ISP 可以提供給您相同的 IP 位址，不論您何時提出要求。您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。

**WAN IP 別名** - 如果您有數個真實 IP 位址且想要在 WAN 介面上使用，請使用此功能。除了目前使用的這一組之外，您還可以設定多達 8 組的真實 IP 位址。

http://192.168.1.5 - WAN IP Alias - Microsoft Internet Explorer

WAN IP Alias ( Multi-NAT )

| Index | Enable | Aux. WAN IP | Join NAT IP Pool |
|---|---|---|---|
| 1. | v | 172.16.3.229 | v |
| 2. | ☐ | | ☐ |
| 3. | ☐ | | ☐ |
| 4. | ☐ | | ☐ |
| 5. | ☐ | | ☐ |
| 6. | ☐ | | ☐ |
| 7. | ☐ | | ☐ |
| 8. | ☐ | | ☐ |

OK Clear All Close

**固定 IP 位址** – 按**是**使用此功能並輸入一個固定的 IP 位址。
**預設MAC位址** – 您可以使用預設MAC位址或是在此區域中填入另一組位址。
**指定 MAC 位址** – 手動輸入路由器的 MAC 位址。

在您完成上述的設定之後，請按**確定**按鈕來啓動設定。

### 3.1.3 固定或動態 IP

對固定 IP 模式來說，通常您會收到 DSL 或是 ISP 服務供應商提供給您的一個固定的真實 IP 位址或是真實子網路，在大多數的情形下，Cable 服務供應商將會提供一個固定的真實 IP，而 DSL 服務供應商提供的是真實子網路資料。如果您有一組真實的子網路，您可以指派一組或是多組 IP 位址至 WAN 介面。

若要使用**固定或動態 IP** 爲網際網路的連線協定，請自 **Internet Access** 中選擇**固定或動態 IP**，即可出現下圖。

Internet Access >> Static or Dynamic IP

Static or Dynamic IP (DHCP Client)

Access Control
Broadband Access ⦿ Enable ○ Disable

Keep WAN Connection
☐ Enable PING to keep alive
PING to the IP 0.0.0.0
PING Interval 0 minute(s)

WAN physical type
Auto negotiation

WAN Connection Detection
Mode ARP Detect
Ping IP
TTL:

RIP Protocol
☐ Enable RIP

WAN IP Network Settings WAN IP Alias
⦿ Obtain an IP address automatically
Router Name *
Domain Name *
* : Required for some ISPs
○ Specify an IP address
IP Address 192.168.5.26
Subnet Mask 255.255.255.0
Gateway IP Address 192.168.5.1

⦿ Default MAC Address
○ Specify a MAC Address
MAC Address:
00 .50 .7F :9A .32 .71

DNS Server IP Address
Primary IP Address
Secondary IP Address

OK

**Access Control** C 按**啓用**以啓動此功能，如果您按的是**停用**，此功能將會關閉，您在此頁面所完成的全部設定都將失效。

**維持 WAN 連線** 正常情況下，這個功能是設計用來符合動態 IP 環境，因爲某些 ISP 會在一段時間沒有任何回應時中斷連線。請勾選**啓用 PING 以保持常態連線**。

**PING 到指定的 IP** – 如果您啓用此功能，請指定 IP 位址讓系統可以 PING 到該 IP 以保持連線

**PING 間隔** - 輸入間隔時間讓系統得以執行 PING 動作。

**WAN 連線檢測** 這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。

模式 – 選擇 **ARP Detect 或 Ping Detect** 執行 WAN 檢測動作。

**Ping IP** – 如果您選擇 **Ping Detect** 作爲檢測模式，您必須在本區輸入 IP 位址作爲 Ping 檢測之用。

**TTL (Time to Live)** – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。

**RIP 協定** 指名路由器是如何變更路由表格資訊，勾選此項目以啓動此功能。

**WAN IP 網路設定** 這個區域允許您自動取得 IP 位址並讓您手動輸入 IP 位址。

**WAN IP 別名** - 如果您有多個真實 IP 位址，想要在 WAN 介面上利用這些 IP，請使用 WAN IP 別名。除了目前使用的 IP 外，您還可以另外設定 8 組真實 IP，要注意的是，本項設定僅針對 WAN1 有效用。

http://192.168.1.5 - WAN IP Alias - Microsoft Internet Explorer

WAN IP Alias ( Multi-NAT )

| Index | Enable | Aux. WAN IP | Join NAT IP Pool |
|---|---|---|---|
| 1. | v | 172.16.3.229 | v |
| 2. | ☐ | | ☐ |
| 3. | ☐ | | ☐ |
| 4. | ☐ | | ☐ |
| 5. | ☐ | | ☐ |
| 6. | ☐ | | ☐ |
| 7. | ☐ | | ☐ |
| 8. | ☐ | | ☐ |

OK  Clear All  Close

**自動取得 IP 位址** – 如果您想要使用**動態 IP** 模式，按此鈕以自動取得 IP 位址。

***路由器名稱***: 輸入 ISP 的路由器名稱。

***網域名稱***: 輸入指定的網域名稱。

**指定 IP 位址** – 按此鈕指定 IP 位址讓資料通過。

***IP 位址***:輸入 IP 位址。

***子網路遮罩***:輸入子網路遮罩。

***閘道 IP 位址***: 輸入閘道 IP 位址。

***預設MAC 位址***: 按此鈕使用預設的 MAC 位址。

***指定MAC 位址***: 部分 Cable 服務供應商會指定 MAC 位址作爲存取驗證之用，此時您需要按下此鈕並在下方區域輸入 MAC 位址。

**DNS 伺服器 IP 位址** 若要使用固定 IP 模式，請輸入路由器的主要 IP 位址，如有必要，在將來，您也可以輸入次要 IP 位址以符合所需。

## 3.1.4 PPTP/L2TP

若要使用 **PPTP/L2TP** 爲網際網路的連線協定，請自 **Internet Access** 中選擇 **PPTP/L2TP**，即可出現下圖。

Internet Access >> PPTP

PPTP Client Mode

| PPTP Setup | | PPP Setup | |
|---|---|---|---|
| PPTP Link | ○ Enable ⊙ Disable | PPP Authentication | PAP or CHAP |
| PPTP Server | | ☑ Always On | |
| ISP Access Setup | | Idle Timeout | -1 second(s) |
| Username | 123 | IP Address Assignment Method (IPCP) | |
| Password | ●●● | Fixed IP | ○ Yes ⊙ No (Dynamic IP) |
| Index(1-15) in Schedule Setup: | | Fixed IP Address | |
| => , , , | | WAN IP Network Settings | |
| | | ○ Obtain an IP address automatically | |
| | | ⊙ Specify an IP address | |
| | | IP Address | 172.16.3.229 |
| | | Subnet Mask | 255.255.0.0 |

OK

**PPTP Setup**

按**啓用**以啓動此功能，如果您按的是**停用**，此功能將會關閉，您在此頁面所完成的全部設定都將失效。

**PPTP Server** – 如果您啓用了 PPTP/L2TP 模式，請指定伺服器的 IP 位址。

**ISP 存取設定**

**使用者名稱** –在本區請輸入 ISP 提供的使用者名稱。

**密碼** – 在本區請輸入 ISP 提供的密碼。

**索引號碼(1-15) 於排程設定** -可以輸入四組時間排程，全部的排程都是在**應用-排程**網頁中事先設定完畢，您可在此輸入該排程的索引編號。

**PPP Setup**

**PPP Authentication** - Select **PAP only** or **PAP or CHAP** for PPP.

**Idle Timeout** - Set the timeout for breaking down the Internet after passing through the time without any action.

**IP 位址指派方式 (IPCP)**

通常每次的連線，ISP 會隨機指派 IP 位址給您，在某些情況下，您的 ISP 可以提供給您相同的 IP 位址，不論您何時提出要求。您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。

**固定 IP 位址** –請輸入一組固定 IP。

**WAN IP 網路設定**

**自動取得 IP 位址** – 如果您想要使用**動態 IP** 模式，按此鈕以自動取得 IP 位址。

**指定 IP 位址** – 按此鈕指定 IP 位址讓資料通過。

***IP 位址***:輸入 IP 位址。

***子網路遮罩***:輸入子網路遮罩。

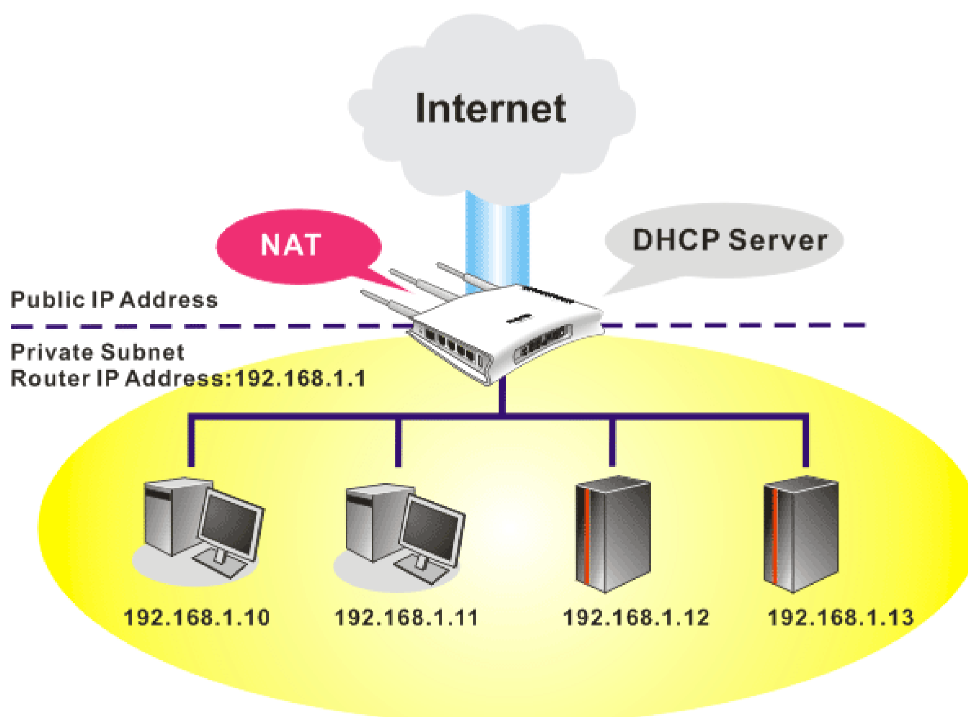
# 3.2 LAN

區域網路是由路由器所管理的一群子網路，網路結構設計和您自 ISP 所取得之真實 IP 位址有關。

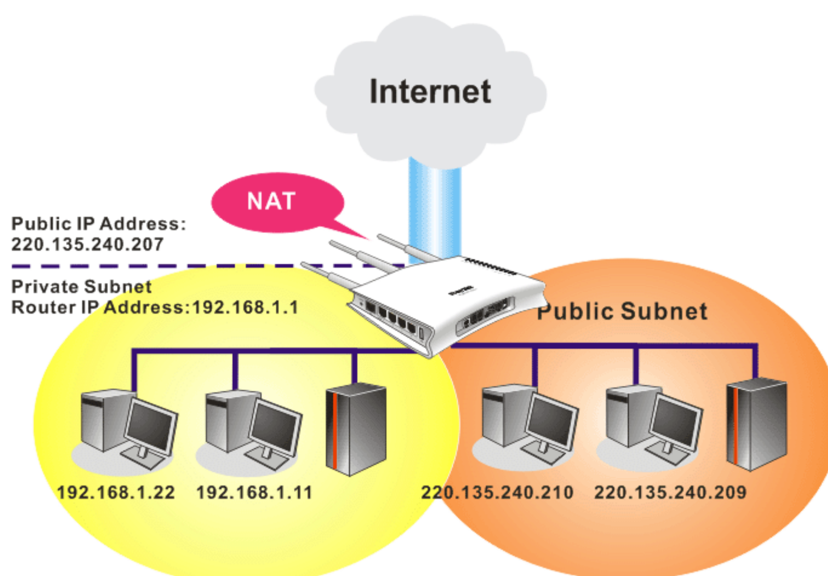
LAN
- General Setup

## 3.2.1 區域網路基本概念

Vigor 路由器最基本的功能爲 NAT，可用來建立虛擬的子網路，如前所述，路由器利用真實 IP 位址與網際網路上其他的真實主機互相通訊，或是使用虛擬 IP 地址與區域網路上的主機連繫。NAT 要完成的事情就是轉換來自真實 IP 位址的封包到私有 IP 地址，以便將正確的封包傳送至正確的主機上，反之亦然。此外 Vigor 路由器還有內建的 DHCP 伺服器，可指定虛擬 IP 地址至每個區域主機上，請參考下面的範例圖，即可獲得大略的了解。




在某些特殊的情形當中，您可能會有 ISP 提供給您的真實 IP 子網路像是 220.135.240.0/24，這表示您可以設定一個真實子網路，或是使用配備有真實 IP地址之主機的第二組子網路，作爲真實子網路的一部份，Vigor 路由器將會提供 IP 路由服務，幫助真實地區子網路上的主機能與其他真實主機/外部伺服器溝通連繫，因此路由器必須設定爲真實主機的通訊閘道才行。




### 什麼是 RIP(Routing Information Protocol)

Vigor 路由器可利用 RIP 與鄰近路由器交換路由資訊，達到 IP 路由的目的。這樣可讓使用者變更路由器的資訊，例如 IP 地址，且路由器還會自動通知雙方此類訊息。

## 3.2.2 基本設定

本頁提供您區域網路的基本設定。

按**區域網路**開啓區域網路設定並選擇**基本設定**。

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

| LAN IP Network Configuration | | DHCP Server Configuration | |
|---|---|---|---|
| For NAT Usage | | ◉ Enable Server ○ Disable Server | |
| 1st IP Address | 192.168.1.5 | Relay Agent: ○ 1st Subnet ○ 2nd Subnet | |
| 1st Subnet Mask | 255.255.255.0 | Start IP Address | 192.168.1.10 |
| For IP Routing Usage ○ Enable ◉ Disable | | IP Pool Counts | 50 |
| 2nd IP Address | 192.168.2.1 | Gateway IP Address | 192.168.1.5 |
| 2nd Subnet Mask | 255.255.255.0 | DHCP Server IP Address for Relay Agent | |
| 2nd Subnet DHCP Server | | DNS Server IP Address | |
| RIP Protocol Control | Disable | ☐ Force DNS manual setting | |
| | | Primary IP Address | |
| | | Secondary IP Address | |

OK

**第一 IP 位址** 請輸入虛擬 IP 地址以便連接區域虛擬網路(預設值爲 192.168.1.1)。

**第一子網路遮罩** 請輸入決定網路大小的位址碼(預設值爲 255.255.255.0/ 24)。

**供 IP 路由使用** 按下**啓用**以啓動此功能，此功能預設值是**停用**。此應用視情況需要而設定。

**第二 IP 位址** 請輸入第二組 IP 地址以便連接至子網路(預設值爲 192.168.2.1)。

**第二子網路遮罩** 請輸入第二組決定網路大小的位址碼(預設值爲 255.255.255.0/ 24)。

**第二子網路遮罩 DHCP 伺服器** 您可以將路由器設定爲 DHCP 伺服器，提供服務予第二組子網路。

http://192.168.1.5 - Router Web Configurator - Microsoft Internet Explorer

2nd DHCP Server

Start IP Address

IP Pool Counts 0 (max. 10)

Index Matched MAC Address given IP Address

MAC Address :

Add Delete Edit Cancel

OK Clear All Close

**起始 IP 位址：**輸入 IP 地址 pool 數值做爲 DHCP 伺服器指定 IP 地址時的起始點，如果路由器的第二組 IP 地址爲 220.135.240.1,，起始 IP 地址可以是 220.135.240.2 或是更高一些，但比 220.135.240.254 小。

**IP 配置數量：**輸入 IP 地址的數量，最大值爲 10，例如您若輸入 3 而第二組 IP 地址爲 220.135.240.1，DHCP 伺服器的 IP 地址範圍即爲 220.135.240.2 到 220.135.240.4。

**MAC 位址：**請一個個輸入主機的 MAC 地址，按**新增**來建立主機清單以便指定、刪除或是編輯上述範圍中的 IP 地址。設定第二組 DHCP 伺服器所需的 MAC 位址清單，可幫助路由器指定正確的 IP 地址及子網路至正確的主機上。這樣在第二子網路上的主機便不會得到屬於第一組子網路的 IP 地址。

**RIP 協定控制** **停用** – 關閉 RIP 協定，可讓不同路由器之間資訊交換暫停 (此爲預設值)。

RIP Protocol Control Disable

Disable
1st Subnet
2nd Subnet

**第一子網路-**選擇路由器以交換第一子網路和鄰近路由器間的

RIP 資訊。
**第二子網路-**選擇路由器以交換第二子網路和鄰近路由器間的 RIP 資訊。

**DHCP 伺服器組態**

DHCP 是 Dynamic Host Configuration Protocol 的縮寫，路由器的出廠預設值可以作為您的網路的 DHCP 伺服器，所以它可自動分派相關的 IP 設定給區域的使用者，將該使用者設定成為 DHCP 的用戶端。如果您的網路上並沒有任何的 DHCP 伺服器存在，建議您讓路由器以 DHCP 伺服器的型態來運作。

如果您想要使用網路上另外的 DHCP 伺服器，而非路由器的伺服器，您可以利用中繼代理來幫您重新引導 DHCP 需求到指定的位置上。
**啓用 -** 讓路由器指定 IP 地址到區域網路上的每個主機上。
**停用 –** 讓您手動指定 IP 地址到區域網路上的每個主機上。
**DHCP 中繼代理位址 - (1st subnet/2nd subnet)**指定某個 DHCP 伺服器所在的子網路讓中繼代理重新引導 DHCP 需求至該處。
**起始 IP 位址 -**輸入 DHCP 伺服器的 IP 地址配置的數值作為指定 IP 地址的起始點，如果第路由器的第一個 IP 地址為 192.168.1.1，起始 IP 地址可以是 192.168.1.2 或是更高一些，但比 192.168.1.254 小。
**IP 配置數量 -**輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值為 50，最大值為 253。
**閘道 IP 位址 -**輸入 DHCP 伺服器所需的閘道 IP 地址，這項數值通常與路由器的第一組 IP 地址相同，表示路由器為預設的閘道。
**DHCP 伺服器 IP 位址關於中繼代理程式 -**設定您預備使用的 DHCP 伺服器 IP 位址，讓中繼代理可以協助傳送 DHCP 需求至伺服器上。

**DNS 伺服器組態**

DNS 是 Domain Name System 的縮寫，每個網際網路的主機都必須擁有獨特的 IP 地址，也必須有人性化且容易記住的名稱諸如 www.yahoo.com 一般，DNS 伺服器可轉換此名稱至相對應的 IP 地址上。

**使用 DNS 手動設定 –** 強迫路由器使用本頁所指定的 DNS 伺服器而非使用網際網路存取伺服器所提供的 DNS 伺服器 (PPPoE, PPTP, L2TP 或 DHCP 伺服器).
**主要 IP 位址 -**您必須在此指定 DNS 伺服器的 IP 地址，因為通常您的 ISP 應該會提供一個以上的 DNS 伺服器，如果您的 ISP 並未提供，路由器會自動採用預設的 DNS 伺服器 IP 地址 194.109.6.66，放在此區域。
**次要 IP 位址 -** 您可以在此指定第二組 DNS 伺服器 IP 位址，因為 ISP 業者會提供一個以上的 DNS 伺服器。如果您的 ISP 並未提供，路由器會自動採用預設的第二組 DNS 伺服器，其 IP 位址為 194.98.0.1，放在此區域。

預設 DNS 伺服器 IP 位址可在線上狀態上查看：

System Status　　System Uptime: 5:11:9

| LAN Status | | Primary DNS: 194.109.6.66 | Secondary DNS: 168.95.1.1 |
|---|---|---|---|
| IP Address | TX Packets | RX Packets | |
| 192.168.1.5 | 9326 | 9487 | |

如果主要和次要 IP 地址區都是空白的，路由器將會指定其本身的 IP 地址給予本地使用者作爲 DNS 代理伺服器並且仍保有 DNS 快速緩衝貯存區。

如果網域名稱的 IP 地址已經在 DNS 快速緩衝貯存區內，路由器將立即 resolve 網域名稱。否則路由器會藉著建立 WAN (例如 DSL/Cable)連線時，傳送 DNS 疑問封包至外部 DNS 伺服器。

第五章中舉出二種常見的區域網路設定腳本供您參考，有關設定範例部份，如有需求請參考該章以取得更多的訊息。

## 3.3 NAT

通常，路由器可以 NAT 路由器提供其相關服務，NAT 是一種機制，一個或多個虛擬 IP 位址可以對應到某個單一的真實 IP 位址。真實 IP 位址習慣上是由您的 ISP 所指定的，因此您必須爲此負擔費用，虛擬 IP 位址則只能在內部主機內辨識出來。

當封包之目的地位址爲網路上某個伺服器時，會先送到路由器，路由器即改變其來源位址，成爲真實 IP 位址，並透過真實通訊埠傳送出去。同時，路由器在連線數表格中列出清單，以記錄位址與通訊埠對應的相關資訊，當伺服器回應時，資料將直接傳回路由器的真實 IP 位址。

NAT 的好處如下：

- **於應用真實 IP 位址上節省花費以及有效利用 IP 位址** NAT 允許本機中的 IP 位址轉成真實 IP 位址，如此一來您可以一個 IP 位址來代表本機。
- **利用隱匿的 IP 位址強化內部網路的安全性** 有很多種攻擊行動都是基於 IP 位址而對受害者發動的，既然駭客並不知曉任何虛擬 IP 位址，那麼 NAT 功能就可以保護內部網路不受此類攻擊。

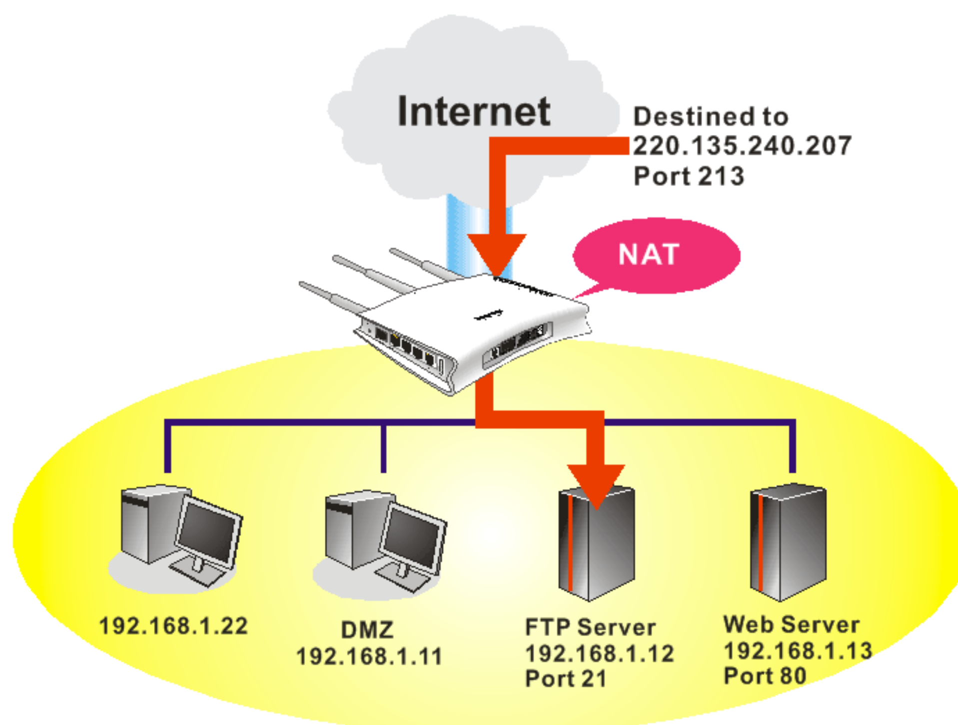
在 NAT 頁面中，您將可看見以 RFC-1918 定義的虛擬 IP 位址，通常我們會使用 192.168.1.0/24 子網路給予路由器使用。就如前所提及的一般，NAT 功能可以對應一或多個 IP 位址和/或服務通訊埠到不同的服務上，換句話說，NAT 功能可以利用通訊埠對應方式來達成。

下圖爲 NAT 功能項目：




### 3.3.1 通訊埠重導向

**通訊埠重導向**通常是爲了本地區域網路中的網頁伺服器、FTP 伺服器、E-mail 伺服器等相關服務而設定，大部分的情形是您需要給每個伺服器一個真實 IP 位址，此一真實 IP 位址/網域名稱可以爲所有使用者所辨識。既然此伺服器實際坐落於區域網路內，因此網路可以受到路由器之 NAT 的詳密保護，且可由虛擬 IP 位址/通訊埠來辨認。通訊埠重導向表的功能是傳送所有來自外部使用者對真實 IP 位址之存取需求，以對應至伺服器的虛擬 IP 位址/通訊埠。




**通訊埠重導向**只能應用在流入的資料量上。

欲使用此項功能，請開啓 **NAT** 頁面然後選擇**通訊埠重導向。通訊埠重導向**提供 20 組通訊埠對應入口給予內部主機對應使用。

NAT >> Port Redirection

Port Redirection | Set to Factory Default |

| Index | Service Name | Public Port | Private IP | Status |
|---|---|---|---|---|
| 1. | | | | x |
| 2. | | | | x |
| 3. | | | | x |
| 4. | | | | x |
| 5. | | | | x |
| 6. | | | | x |
| 7. | | | | x |
| 8. | | | | x |
| 9. | | | | x |
| 10. | | | | x |

<< 1-10 | 11-20 >> Next >>

按下索引編號下的號碼連結，進入次層之設定頁面:

NAT >> Port Redirection

Index No. 1

☐ Enable

| | |
|---|---|
| Mode | Single (Single / Range) |
| Service Name | |
| Protocol | --- |
| WAN IP | 1.All |
| Public Port | 0 |
| Private IP | |
| Private Port | 0 |

Note: In "Range" Mode the End IP will be calculated automatically once the Public Port and Start IP have been entered.

OK Clear Cancel

| | |
|---|---|
| **啓用** | 勾選此方塊啓用此通訊埠重導向設定。 |
| **模式** | 有二種模式可以供使用者選擇，如欲設定範圍給予指定服務，請選擇**範圍**。在"範圍" 模式下，若 IP 位址與第一個對外通訊埠號皆填入之後，系統將自動計算並顯示第二個對外通訊埠值。 |
| **服務名稱** | 輸入特定網路服務的名稱。 |
| **通訊協定** | 選擇傳送層級的通訊協定(TCP 或 UDP)。 |
| **WAN IP** | |
| **對外通訊埠** | 指定哪一個通訊埠可以重新導向至內部主機特定的虛擬 IP 通訊埠上。如果您選擇**範圍**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入需要的數值，系統將會自動指定數值予第二個方塊。 |
| **虛擬 IP** | 指定提供服務的主機之 IP 位址，如果您選擇**範圍**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入完整的 IP 位址 (作爲起點)，在第二個方塊輸入四位數字(作爲終點)。 |
| **虛擬通訊埠** | 指定內部主機提供服務之虛擬通訊埠號。 |

注意路由器有其內建服務(伺服器)諸如 Telnet、HTTP 和 FTP，因爲這些服務(伺服器)的通訊埠號幾乎都相同，因此您可能需要重新啓動路由器以避免衝突發生。

例如，路由器的內建網頁設定給予的設定值是埠號 80，它可能造成與本地網路中網頁伺服器 http://192.168.1.13:80 產生衝突，因此您需要改變路由器的 **http** 通訊埠號，除了 80 以外任何一種都可以（例如 8080），來防止衝突發生。在系統管理群中的管理設定可以做此調整，接著您可在 IP 位址尾端加入 8080 (如 http://192.168.1.1:8080 而非僅只通訊埠號 80)來進入管理畫面。

系統維護 >> 管理

管理設定

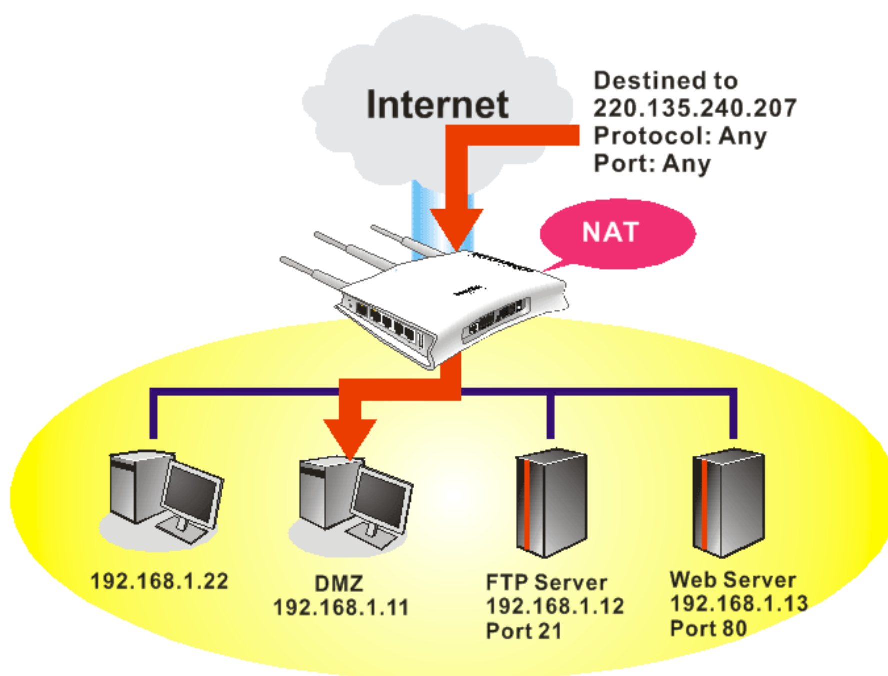
| 管理存取控制 | 管理通訊埠設定 |
|---|---|
| ☑ 允許從網際網路管理 | ◉ 使用者定義通訊埠 ○ 預設通訊埠 |
| ☐ FTP 通訊埠 | Telnet 通訊埠 23 (Default: 23) |
| ☑ HTTP 通訊埠 | HTTP 通訊埠 80 (Default: 80) |
| ☑ HTTPS 通訊埠 | HTTPS 通訊埠 443 (Default: 443) |
| ☑ Telnet 通訊埠 | FTP 通訊埠 21 (Default: 21) |
| ☐ SSH 通訊埠 | SSH 通訊埠 22 (Default: 22) |
| ☑ 斷絕來自外部網際網路的PING | |

| 存取清單 | | | SNMP 設定 | |
|---|---|---|---|---|
| 清單 | IP | 子網路遮罩 | ☐ 啟用 SNMP 代理程式 | |
| 1 | | | 取得社群(Get Community) | public |
| 2 | | | 設定社群(Set Community) | private |
| 3 | | | 管理者主機 IP | |
| | | | 封鎖社群(Trap Community) | public |
| | | | 通知主機 IP | |
| | | | 封鎖逾時 | 10 秒 |

確定

## 3.3.2 DMZ 主機設定

如同上面所提及的內容，通訊埠重導向可以將流入的 TCP/UDP 或是特定通訊埠中其他的流量，重新導向區域網路中特定主機之 IP 位址/通訊埠。不過其他的 IP 協定例如協定 50 (ESP)和 51(AH)是不會在固定通訊埠上行動的，Vigor 路由器提供一個很有效的工具 DMZ 主機，可以將任何協定上的需求資料對應到區域網路的單一主機上。來自用戶端的正常網頁搜尋和其他網際網路上的活動將可繼續進行，而不受到任何打擾。DMZ 主機允許內部被定義規範的使用者完全暴露在網際網路上，通常可促進某些特定應用程式如 Netmeeting 或是網路遊戲等等的進行。




> **注意**：NAT 固有的安全性屬性在您設定 DMZ 主機時稍微被忽略了，建議您另外新增額外的過濾器規則或是第二組防火牆。

請按 **DMZ 主機設定**開啓下述頁面：

NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

None

Private IP　　Choose PC

MAC Address of the True IP DMZ Host　00 . 00 . 00 : 00 . 00 . 00

Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on.

OK

如果您在**網際網路連線設定**選擇 **PPPoE/固定 IP/PPTP**，並且設定 **WAN 別名，**您將可在此頁面發現**輔助 WAN IP** 項目。

NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

| Index | Enable | Aux. WAN IP | Private IP | |
|---|---|---|---|---|
| 1. | ☐ | 172.16.3.229 | | Choose PC |
| 2. | ☐ | 162.168.1.55 | | Choose PC |

OK　Clear

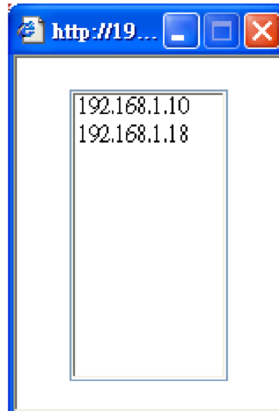
**開啓**　　勾選此項以啓動 DMZ 主機功能。

**虛擬 IP**

輸入 DMZ 主機的虛擬 IP 位址，或是按**選擇 PC** 開啓另一頁面來選擇。

**選擇電腦**

按下此鈕後，如下視窗立即跳出。此視窗包含您的區域網路中全部主機的虛擬 IP 位址清單，請自清單中選擇一個虛擬 IP 位址作爲 DMZ 主機。




當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下面的螢幕上，請按**確定**儲存這些設定。

NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

| Index | Enable | Aux. WAN IP | Private IP | |
|---|---|---|---|---|
| 1. | ☑ | 172.16.3.229 | 192.168.1.10 | Choose PC |
| 2. | ☐ | 162.168.1.55 | | Choose PC |

OK　Clear

### 3.3.3 開放通訊埠

**開放通訊埠**允許您開啓一段範圍內的通訊埠，供特定應用程式使用。常見的應用程式包含有 P2P 應用程式(如 BT、KaZaA、Gnutella、WinMX、eMule 和其他)、Internet Camera 等等，您需要先確定應用程式包含最新的資料，以免成爲安全事件的受害者。

按**開放通訊埠**連結開啓下面的網頁。

NAT >> Open Ports

Open Ports Setup | Set to Factory Default |

| Index | Comment | Aux. WAN IP | Local IP Address | Status |
|---|---|---|---|---|
| 1. | | | | x |
| 2. | | | | x |
| 3. | | | | x |
| 4. | | | | x |
| 5. | | | | x |
| 6. | | | | x |
| 7. | | | | x |
| 8. | | | | x |
| 9. | | | | x |
| 10. | | | | x |

<< 1-10 | 11-20 >> Next >>

**索引** 表示本地主機中您想要提供之服務，其特定內容網頁之相關號碼，您應該選擇適當的索引號碼以編輯或是清除相關的內容。

**註解** 指定特定網路服務的名稱。

**內部 IP 位址** 顯示提供此項服務之本地主機的 IP 位址。

**狀態** 顯示每項設定的狀態，X 或 V 表示關閉或是啓用狀態。

如果要新增或是編輯通訊埠設定，請按索引下方的號碼按鈕。該索引號碼入口設定頁面隨即出現，在每個輸入頁面中，您可以指定 10 組通訊埠範圍給予不同的服務。

NAT >> Open Ports >> Edit Open Ports

Index No. 1

☑ Enable Open Ports

| | |
|---|---|
| Comment | P2P |
| WAN IP | 172.16.3.229 |
| Local Computer | 192.168.1.10 [Choose PC] |

| | Protocol | Start Port | End Port | | Protocol | Start Port | End Port |
|---|---|---|---|---|---|---|---|
| 1. | TCP | 4500 | 4700 | 6. | ----- | 0 | 0 |
| 2. | UDP | 4500 | 4700 | 7. | ----- | 0 | 0 |
| 3. | ----- | 0 | 0 | 8. | ----- | 0 | 0 |
| 4. | ----- | 0 | 0 | 9. | ----- | 0 | 0 |
| 5. | ----- | 0 | 0 | 10. | ----- | 0 | 0 |

OK Clear Cancel

**啓用開放通訊埠** 勾選此項以啓動此功能。

**說明** 請爲所定義的網路應用/服務命名。

**WAN 介面** 指定該項設定之 WAN 介面。

**WAN IP** 如果您在**網際網路連線設定**選擇 **PPPoE/固定 IP/PPTP**，並且設定 **WAN 別名**，您將可在此頁面發現 **WAN IP** 項目。請自下拉式選項中選擇需要的 IP 位址。

**本機電腦** 輸入本機的虛擬 IP 位址或是按**選擇電腦**挑選另外一個。

**選擇電腦** 按此鈕後另一個視窗即自動跳出並提供本機的虛擬 IP 位址之清單資料，請自清單中選取最適宜的 IP 位址。

**通訊協定** 指定傳送層級的通訊協定，有 **TCP**、**UDP** 和 **----- (none)**等幾種選擇。

**起始通訊埠** 指定本機所提供之服務的開始通訊埠號。

**結束通訊埠** 指定本機所提供之服務的結束通訊埠號。

## 3.4 其他應用

下圖顯示**應用**的功能項目：




### 3.4.1 動態 DNS

當您透過 ISP 業者嘗試連接到網際網路時，ISP 業者提供的經常是一個浮動 IP 位址，這表示指派給您的路由器使用之真實 IP 位址每次都會有所不同，DDNS 可讓您指派一個網域名稱給予浮動廣域網路 IP 位址。它允許路由器線上更新廣域網路 IP 位址，以便對應至特定的 DDNS 伺服器上。一旦路由器連上網路，您將能夠使用註冊的網域名稱，並利

用網際網路存取路由器或是內部虛擬的伺服器資料。如果您的主機擁有網路伺服器、FTP 伺服器或是其他路由器後方提供的伺服器，這項設定就特別有幫助也有意義。

在您使用 DDNS 時，您必須先向 DDNS 服務供應商要求免費的 DDNS 服務，路由器提供分別來自不同 DDNS 服務供應商的三種帳號。基本上，Vigor 路由器和大多數的 DDNS 服務供應商 **www.dyndns.org, www.no-ip.com**、**www.dtdns.com**、**www.changeip.com**、**www.dynamic-nameserver.com** 像是都能相容，您應該先造訪其網站為您的路由器註冊自己的網域名稱。

**啓動此功能並增加一個動態 DNS 帳戶**

1. 假設您已經從 DDNS 供應商註冊了一個網域名稱(例如 hostname.dyndns.org)，且獲得一個帳號，其使用者名稱為 *test*；密碼為: *test*。
2. 自**應用**群組選擇**動態 DNS** 設定，下述頁面即會出現在螢幕上。

Applications >> Dynamic DNS Setup

Dynamic DNS Setup | Set to Factory Default |

☐ Enable Dynamic DNS Setup [View Log] [Force Update]

Accounts:

| Index | Domain Name | Active |
|---|---|---|
| 1. | . | x |
| 2. | . | x |
| 3. | . | x |

[OK] [Clear All]

| | |
|---|---|
| **回復出廠預設值** | 清除全部設定資料並回復到出廠的設定。 |
| **啓用動態 DNS 設定** | 勾選此方塊啓用此功能。 |
| **索引** | 按下方的號碼連結進入 DDNS 設定頁面，以設定帳戶。 |
| **網域名稱** | 顯示您在 DDNS 設定頁面上所設定的網域名稱。 |
| **啓用** | 顯示此帳號目前是啓用或是停用狀態。 |
| **檢視記錄** | 可開啓另一個對話盒並顯示 DDNS 資訊紀錄。 |
| **強迫更新** | 按此按鈕強迫路由器取得最新的 DNS 資訊。 |

3. 選擇索引號碼 1，為您的路由器新增一個帳號。勾選**啓用動態 DNS 帳號**，然後選擇正確的服務供應商(例 dyndns.org)，輸入註冊的主機名稱(例 hostname)，並於網域名稱區塊中輸入網域的字尾名稱(例 dyndns.org)；接著輸入您的帳號登入名稱(例 dray)和密碼(例 test)。

Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup

Index : 1

☑ Enable Dynamic DNS Account

Service Provider: dyndns.org (www.dyndns.org)

Service Type: Dynamic

Domain Name: chronic6853 . dyndns.org dyndns.org

Login Name: chronic6853 (max. 64 characters)

Password: ●●●●●●●●●●●● (max. 23 characters)

☐ Wildcards

☐ Backup MX

Mail Extender

OK Clear Cancel

**啓用動態 DNS 帳號** 勾選此方塊以啓用目前帳號，如果您勾選此方塊，您可在步驟 2 中的網頁上看到啓動欄位出現勾選標示。

**服務供應商** 爲此 DDNS 帳號選擇適當的服務供應商。

**服務類型** 選擇服務類型(動態、自訂、固定)。如果您選擇的是**自訂**，您可以修正網域名稱區域中所選定的網域資料。

**網域名稱** 輸入您所申請的網域名稱。請使用下拉式選項選擇想要使用的一個名稱。

**登入名稱** 輸入您在申請網域名稱時所設定之登入名稱。

**密碼** 輸入您在申請網域名稱時所設定之密碼。

**郵件延伸程式** 某些 DDNS 伺服器可能會要求提供額外的資訊，如電子郵件地址，請您在此輸入必要的電子郵件地址，以配合該 DDNS 伺服器之需要。

4. 按**確定**按鈕啓動此設定，您將會看到所做的設定已被儲存。

**萬用字元**與**備份 MX** 並非所有的動態 DNS 服務商都有支援，有關此部分內容，請您自服務商的網站上取得更詳盡的資訊。

**關閉此功能並清除全部動態 DNS 帳號**

取消勾選**啓用動態 DNS 帳號**，並按下**清除全部**按鈕停用此功能以及清除路由器內所有的帳號。

**刪除動態 DNS 帳號**

在**動態 DNS 設定**頁面上，請按您想要刪除之帳號的索引號碼，然後按**清除全部**按鈕即可刪除該帳號。

### 3.4.2 UPnP

**UPnP** 協定爲網路連線裝置提供一個簡易安裝和設定介面，爲 Windows 隨插即用系統上的電腦週邊設備提供一個直接連線的方式。使用者不需要手動設定**通訊埠對應**或是 **DMZ**，**UPnP** 只在 Windows XP 系統下可以運作，路由器提供相關的支援服務給 MSN Messenger，允許完整使用聲音、影像和訊息特徵。

Applications >> UPnP

UPnP

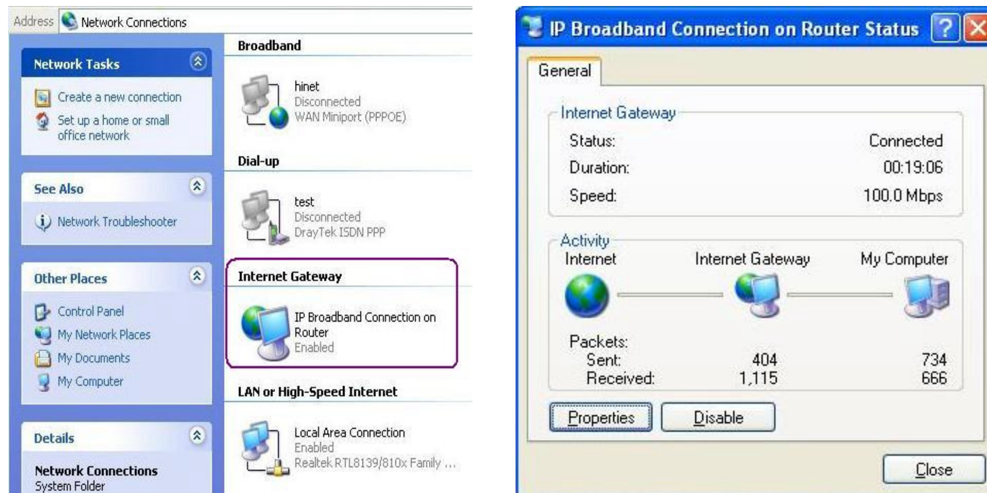
- [x] Enable UPnP Service
  - [ ] Enable Connection control Service
  - [ ] Enable Connection Status Service

Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

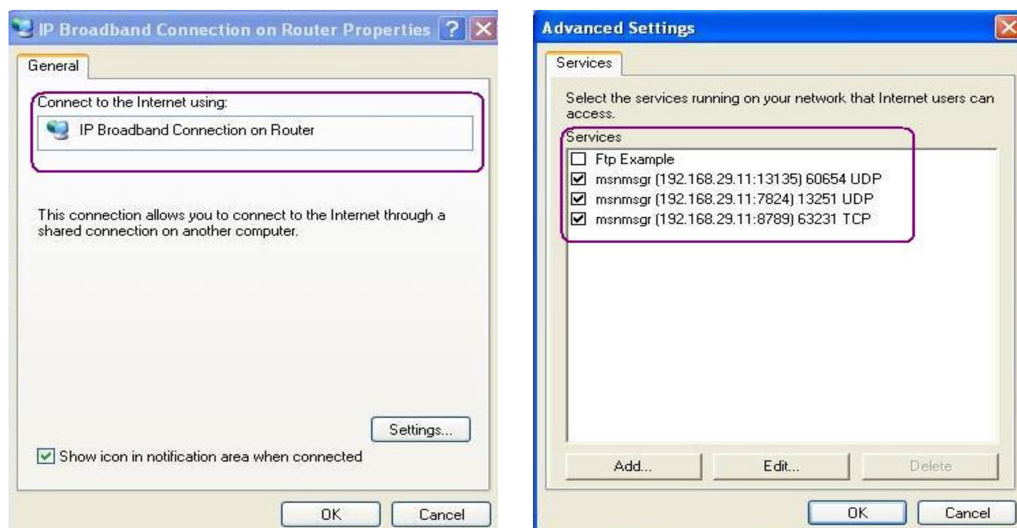
OK Clear Cancel

**啓用 UPnP 服務** 您可以視情況勾選**啓用連線控制服務**或是**啓用連線狀態服務**。

在設定**啓用 UPNP 服務**後，在 Windows XP/網路連線上會出現一個 **IP Broadband Connection on Router** 圖示，連線狀態和控制狀態將可開啓使用，NAT Traversal of UPnP 可啓動應用程式中的多媒體特徵，必須手動設定通訊埠對應或是使用其他類似的方法來設定，以下顯示此項功能的範例圖形。




在路由器上的 UPnP 功能，允許應用程式(像是 MSN Messenger, 可察覺出 UPnP 功能) 找到隱藏在 NAT 路由器之下的是什麼，此應用程式也會記住外部 IP 位址並且在路由器上設定通訊埠對應，結果這種能力可將封包自路由器的外部通訊埠傳送到應用程式所使用的內部通訊埠。




有關防火牆與 UPnP 功能之提示–

**無法與防火牆軟體配合**

在您的電腦上啓用防火牆有可能造成 UPnP 不正常運作，這是因爲這些應用程式會擋掉某些網路通訊埠的存取能力。

**安全考量**

在您的網路上啓用 UPnP 功能可能會招致安全威脅，在您啓用 UPnP 功能之前您應該要小心考慮這些風險。

- 某些微軟操作系統已發現到 UPnP 的缺點，因此您需要確定已經應用最新的服務封包。
- 未享有特權的使用者可以控制某些路由器的功能，像是移除和新增通訊埠對應等。

UPnP 功能可不斷變化的新增通訊埠對應來表示一些察覺 UPnP 的應用程式，當這些應用程式不正常的運作中止時，這些對應可能無法移除。

## 3.5 VoIP

Voice over IP network (VoIP)可讓您使用寬頻網際網路連線撥打網路電話。

有很多種不同的電話信號協定、方法可讓 VoIP 裝置使用以便與對方溝通聯繫，最普遍的協定有 SIP、MGCP、Megaco 和 H.323，這些協定彼此都不完全相容(除非是透過軟體伺服器的掌控)。

Vigor V 系列機種支援 SIP 協定，因爲此種協定對 ITSP (Internet Telephony Service Provider)而言是很理想也很方便，支援也最廣。SIP 是一種端對端信號協定，可建立使用者於 VoIP 結構中之出席情形和機動性。每個想要使用 SIP 相同資源辨識器之用戶都可使用標準的 SIP URI 格式

**sip: user:password @ host: port**

某些區域可能有不同的使用方式，一般來說主機指的是網域，使用者資訊包含有使用者名稱區、密碼區，@符號則緊跟在後，這種格式和 URL 很相似，所以有些人以 SIP URL 來稱呼它。SIP 支援點對點直接撥號，同時也可透過 SIP 代理伺服器(角色雷同 H.323

Gatekeeper)來撥號，而 MGCP 協定則是使用用戶-伺服器結構，撥號方式和目前 PSTN 網路是相同的。

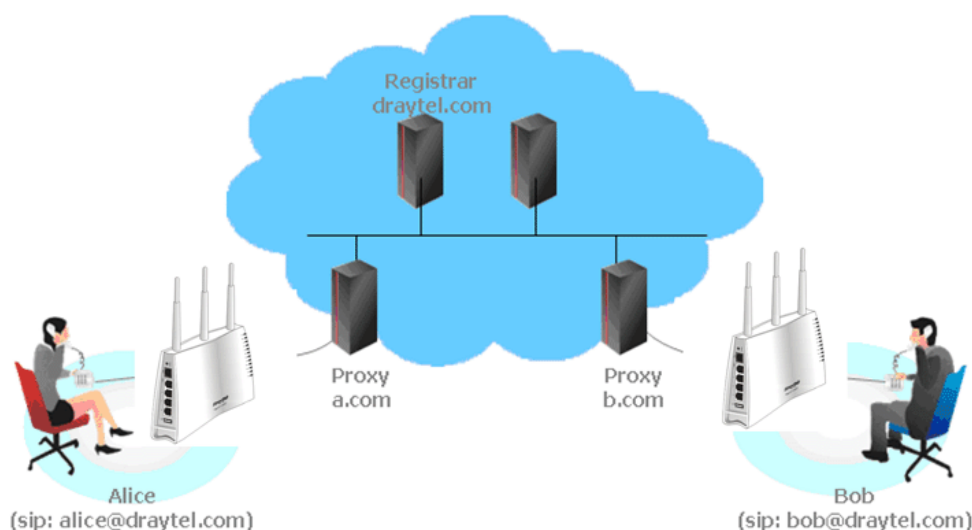
在撥號設定之後，聲音是透過 RTP (Real-Time Transport Protocol)來傳送的，不同的 codecs(用來壓縮和解壓縮聲音)可以包覆於 RTP 封包中，Vigor V 機種提供不同的 codecs 包括 G.711 A/μ-law, G.723, G.726 和 G.729 A & B，每個 codecs 都使用不同頻寬，因此可以提供不同等級的聲音品質。Codec 使用的頻寬越多，聲音品質越好，雖然如此還是應該配合您的網際網路頻寬選擇適宜的 codec 才恰當。

通常有二種撥號類型，說明如下：

- **透過 SIP 伺服器撥號**

  首先 Vigor V 機種必須先向 SIP 註冊，傳送註冊訊息才可生效，然後雙方的 SIP 代理商將轉送一系列訊息給與撥號者，以便建立完整的 session。

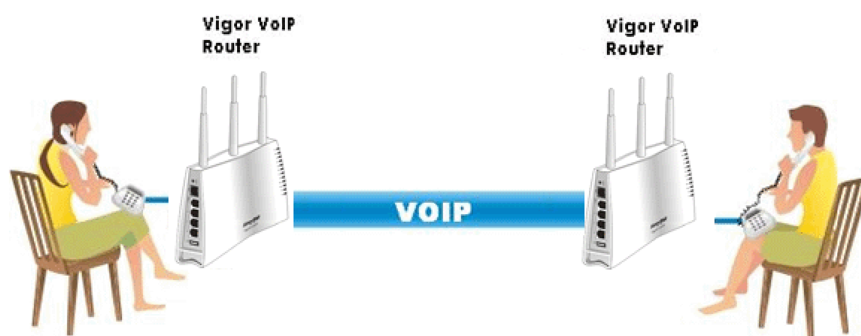
  如果雙方都向相同 ISP 業者註冊，那麼我們可以下圖來做簡單說明：




  這種模式最主要的好處是您不必去記朋友的 IP 位址(因為它可能常常會改變，如果該位址是浮動的位址的話)，相反的您只要使用撥號計畫或是直接撥朋友的帳號名稱就可以了。

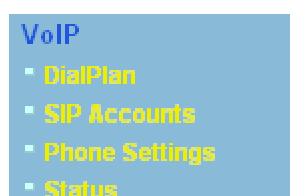
- **點對點**

  我們的 Vigor V 機種首先採用有效之 codecs，但同時也擔保自動 QoS 的功能，QoS 擔保可以協助指定聲音流量較高之優先權，您對聲音所需求之 inbound 和 outbound 頻寬永遠擁有優先處理權，但是您的資料處理就會有些慢，不過還在忍受範圍內。




我們的 Vigor V 機種首先採用有效之 codecs，但同時也擔保自動 QoS 的功能，QoS 擔保可以協助指定聲音流量較高之優先權，您對聲音所需求之 inbound 和 outbound 頻寬永遠擁有優先處理權，但是您的資料處理就會有些慢，不過還在忍受範圍內。

下圖為 VoIP 的功能項目：




### 3.5.1 撥號對應表

本頁讓使用者設定 VoIP 功能所需的電話簿及數字對應設定。請按頁面上的連結進入下一層設定頁面。

VoIP >> DialPlan Setup

DialPlan Configuration

| Phone Book |
| --- |
| Digit Map |
| Call Barring |
| Regional |
| PSTN Setup |

#### 電話簿

在本節中，您可以設定 VOIP 電話，這個設定可以幫助用戶以最快且最簡單的方式撥出電話號碼。本頁總共提供 60 組號碼給用戶儲存朋友以及家人的 SIP 位址。

VoIP >> DialPlan Setup

Phone Book

| Index | Phone number | Display Name | SIP URL | Dial Out Account | Loop through | Backup Phone Number | Status |
|---|---|---|---|---|---|---|---|
| 1. | | | | Default | None | | x |
| 2. | | | | Default | None | | x |
| 3. | | | | Default | None | | x |
| 4. | | | | Default | None | | x |
| 5. | | | | Default | None | | x |
| 6. | | | | Default | None | | x |
| 7. | | | | Default | None | | x |
| 8. | | | | Default | None | | x |
| 9. | | | | Default | None | | x |
| 10. | | | | Default | None | | x |
| 11. | | | | Default | None | | x |
| 12. | | | | Default | None | | x |
| 13. | | | | Default | None | | x |
| 14. | | | | Default | None | | x |
| 15. | | | | Default | None | | x |
| 16. | | | | Default | None | | x |
| 17. | | | | Default | None | | x |
| 18. | | | | Default | None | | x |
| 19. | | | | Default | None | | x |
| 20. | | | | Default | None | | x |

<< 1-20 | 21-40 | 41-60 >> Next >>

Status: v --- Active, x --- Inactive, ? --- Empty

按任何一個索引標號進入下一個設定頁面。

VoIP >> DialPlan Setup

Phone Book Index No. 1

☑ Enable

| | |
|---|---|
| Phone Number | 1 |
| Display Name | Polly |
| SIP URL | 1112 @ fwd.pulver.com |
| Dial Out Account | Default |
| Loop through | None |
| Backup Phone Number | |

OK Clear Cancel

**啓用** 勾選此方塊啓用此號碼。

**電話號碼** 此索引編號的快速撥號號碼，任何號碼都可以使用，範圍是數字 **0-9** 以及 *****。

**顯示名稱** 您想要在朋友的電話螢幕上顯示出來的名稱，可讓您的朋友容易知道是誰打的電話。

**SIP URL** 請輸入朋友的 SIP 位址。

## 數字對應設定

爲了使用者的方便，本頁允許使用者以新號碼來編輯 SIP 帳號的前置號碼，或是取代該號碼等等，這個設定可以提供用戶一個透過 VoIP 介面快速且簡單的撥號方式。

VoIP >> DialPlan Setup

Digit Map Setup

| # | Enable | Prefix Number | Mode | OP Number | Min Len | Max Len | Interface |
|---|---|---|---|---|---|---|---|
| 1 | ☑ | 03 | Replace | 8863 | 7 | 9 | PSTN |
| 2 | ☑ | 886 | Strip | 886 | 8 | 10 | PSTN |
| 3 | ☐ | | None | | 0 | 0 | PSTN |
| 4 | ☐ | | None | | 0 | 0 | PSTN |
| 5 | ☐ | | None | | 0 | 0 | PSTN |
| 6 | ☐ | | None | | 0 | 0 | PSTN |
| 7 | ☐ | | None | | 0 | 0 | PSTN |
| 8 | ☐ | | None | | 0 | 0 | PSTN |
| 9 | ☐ | | None | | 0 | 0 | PSTN |
| 10 | ☐ | | None | | 0 | 0 | PSTN |
| 11 | ☐ | | None | | 0 | 0 | PSTN |
| 12 | ☐ | | None | | 0 | 0 | PSTN |
| 13 | ☐ | | None | | 0 | 0 | PSTN |
| 14 | ☐ | | None | | 0 | 0 | PSTN |
| 15 | ☐ | | None | | 0 | 0 | PSTN |
| 16 | ☐ | | None | | 0 | 0 | PSTN |
| 17 | ☐ | | None | | 0 | 0 | PSTN |
| 18 | ☐ | | None | | 0 | 0 | PSTN |
| 19 | ☐ | | None | | 0 | 0 | PSTN |
| 20 | ☐ | | None | | 0 | 0 | PSTN |

Note: Min Len and Max Len should be between 0~25.

OK Cancel

**啓用** 按此方塊啓動此功能。

**前置號碼** 此處所設定的號碼可用來新增，取代變更之號碼。

**模式**

**無** – 無動作。

**新增** -當您選擇此模式時，變更號碼將會增加前置號碼於前面，並藉由選定的 VoIP 介面撥出。

**卸除** -當您選擇此模式時，變更號碼將會被刪除。

**取代**- 當您選擇此模式時，透過指定的 VoIP 介面之變更號碼將會被前置號碼所取代

模式

無

無
新增
卸除
取代

| | |
|---|---|
| **變更號碼** | 您在此處所輸入的號碼是您想要執行特殊功用的帳號前半部份(依據選擇的模式而定)。 |
| **最小長度** | 設定撥號的最小長度以套用前置號碼之設定，參考上圖所示，如果號碼介於 7 和 9，那麼該號碼可以就能套用此處所設定的前置號碼設定。 |
| **最大長度** | 設定撥號的最大長度以套用前置號碼之設定。 |
| **介面** | 請自預設的六組 SIP 帳號中選擇一個您想要啓動前置號碼設定的介面。 |

## 3.5.2 SIP 帳號

在此頁面中，您可以調整自己的 SIP 設定，當您申請一個帳號時，您的 ISP 服務供應商會給您一個帳號名稱或是使用者名稱、SIP 登錄者、代理人和網域名稱(最後三種在某些條件下，有可能是完全相同的)，您可以告訴您的成員有關您的 SIP 位址，表示法爲**帳號名稱@網域名稱**。

當路由器打開時，將以使用帳號名稱@網域名稱來登錄，之後，您的電話將由 SIP 代理者以帳號名稱@網域名稱傳送至目的地作爲辨識之用。

VoIP >> SIP Accounts

SIP Accounts List

Refresh

| Index | Profile | Domain/Realm | Proxy | Account Name | Ring Port | Status |
|---|---|---|---|---|---|---|
| 1 | | | | --- | ☐Phone1 ☐Phone2 | - |
| 2 | | | | --- | ☐Phone1 ☐Phone2 | - |
| 3 | | | | --- | ☐Phone1 ☐Phone2 | - |
| 4 | | | | --- | ☐Phone1 ☐Phone2 | - |
| 5 | | | | --- | ☐Phone1 ☐Phone2 | - |
| 6 | | | | --- | ☐Phone1 ☐Phone2 | - |

R: success registered on SIP server
-: fail to register on SIP server

NAT Traversal Setting

| | |
|---|---|
| STUN Server: | |
| External IP: | |
| SIP PING Interval: | 150 sec |

OK

| | |
|---|---|
| **索引** | 按此鈕進入下一層設定頁面設定 SIP 帳號。 |
| **設定檔** | 顯示帳號的設定檔名稱。 |
| **網域** | 顯示 SIP 註冊伺服器的網域名稱或是 IP 位址。 |
| **伺服器** | 顯示 SIP 伺服器的網域名稱或是 IP 位址。 |
| **帳號名稱** | 顯示@前面的 SIP 位址帳號名稱。 |
| **振鈴通訊埠** | 指定接收電話時由哪一個通訊埠響鈴。 |
| **STUN 伺服器** | 輸入 STUN 伺服器的 IP 位址或是網域。 |
| **外部 IP** | 輸入閘道 IP 位址。 |

| | |
|---|---|
| **SIP PING 間隔** | 預設值爲 150 秒，對 Nortel 伺服器而言這項設定是相當有用的。 |
| **狀態** | 顯示相關 SIP 帳號的狀態，**R** 表示此帳號已註冊成功，**–** 表示尚未成功註冊。 |

VoIP >> SIP Accounts

SIP Account Index No. 1

| | |
|---|---|
| Profile Name | (11 char max.) |
| Register via | None ☐ Call without Registration |
| SIP Port | 5060 |
| Domain/Realm | (63 char max.) |
| Proxy | (63 char max.) |
| ☐ Act as outbound proxy | |
| Display Name | (23 char max.) |
| Account Number/Name | --- (63 char max.) |
| ☐ Authentication ID | (63 char max.) |
| Password | (63 char max.) |
| Expiry Time | 1 hour 3600 sec |
| NAT Traversal Support | None |
| Ring Port | ☐Phone 1 ☐Phone 2 |
| Ring Pattern | 1 |

OK Cancel

| | |
|---|---|
| **設定檔名稱** | 指定一個名稱作爲辨識之用，您可以使用與網域類似的名稱，例如網域名稱爲 *draytel.org*,您就可以在本區中設定 *draytel-1*。 |
| **由此註冊** | 指定您申請註冊時所透過的介面爲何，如果您不想註冊個人資料而直接使用 VoIP 撥號功能，請選擇**無**。某些 SIP 伺服器允許使用者不須登錄即可使用 VoIP 功能，針對這類伺服器，請您選擇**自動**，系統將爲您選擇最佳方式作爲 VoIP 撥號之用。<br>None<br>None<br>Auto<br>WAN1<br>LAN/VPN |
| **SIP 通訊埠** | 通訊埠號用來傳送/接收 SIP 訊息以建立通訊，雖然預設值爲 5060，您仍可將之變更爲其他數字。不過在這種情形下，還需要對方也同時變更爲相同的數字才行。這時 |
| **網域** | 輸入註冊 SIP 伺服器的網域名稱或 IP 位址。 |
| **伺服器** | 您可以輸入 SIP 代理伺服器的 IP 位址(或網域名稱如 iptel.org)，所有在上述的**網域**區域中指定的訊息來說 Vigor 路由器將之傳送至代理者，由代理者來轉送此訊息。您可以在網域名稱後面輸入通訊埠號，指定該埠號爲資料傳輸的目的地（例如 nat.draytel.org**:5065)。** |

| | |
|---|---|
| **以對外伺服器之身份來運作** | 勾選此方塊以啓用伺服器成爲對外伺服器。 |
| **顯示名稱** | 您想要在朋友的電話顯示螢幕上出現的名稱。 |
| **帳號名稱/號碼** | 輸入 SIP 位址的帳號名稱，例如@之前的文字。 |
| **驗證 ID 身分** | 勾選此方塊啓用此功能並輸入名稱或號碼供 SIP 驗證，如果設定值與帳戶名稱相同，您就不必勾選此方塊另設數值。 |
| **密碼** | 當您以 SIP 服務註冊時所需提供的密碼。 |
| **有效時間** | 爲 SIP 伺服器提保存使用者註冊帳號的有效時間。在到期之前，路由器將會再次傳送另一個註冊需求給予 SIP 登錄伺服器。 |
| **NAT 穿透** | 如果路由器(寬頻路由器)是透過其他裝置連接上網際網路，您就必須設定此功能。<br>NAT Traversal Support [None] None / Stun / Manual / Nortel<br>**無 –**.關閉此功能。<br>**Stun** –若路由器支援 Stun 伺服器，請選擇此項目。<br>**手動** –若您想要指定外部 IP 位址作爲 NAT transversal 支援，請選擇此項目。<br>**Nortel** – 如果軟體支援 nortel 方案，您可以選擇此項目。 |
| **振鈴通訊埠** | 設定 VoIP 1,VoIP 2 作爲 SIP 帳號的預設振鈴通訊埠。 |
| **振鈴樣式** | **選擇** VoIP 電話的振鈴樣式。<br>Ring Pattern [1] 1 / 2 / 3 / 4 / 5 / 6 |

## 3.5.3 P 電話設定

本頁讓使用者得以個別設定 VoIP 1 和 VoIP 2 。

VoIP >> Phone Settings

**Phone List**

| Index | Port | Call Feature | Codec | Tone | Gain (Mic/Speaker) | Default SIP Account | DTMF Relay |
|---|---|---|---|---|---|---|---|
| 1 | Phone1 | CW,CT, | G.729A/B | User Defined | 5/5 | | InBand |
| 2 | Phone2 | CW,CT, | G.729A/B | User Defined | 5/5 | | InBand |

**RTP**

☐ Symmetric RTP

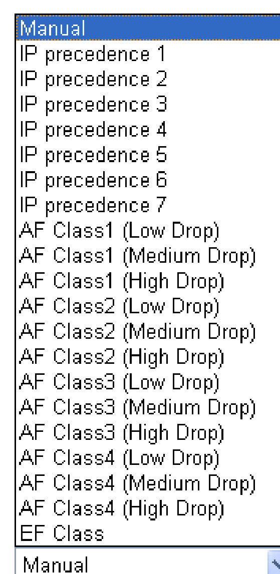
Dynamic RTP Port Start 10050

Dynamic RTP Port End 15000

RTP TOS IP precedence 5 10100000

OK

| | |
|---|---|
| **電話清單** | **通訊埠** – 有種通訊埠類型提供給您選擇。<br>**通話功能** – 這個欄位簡單描述此通電話的功能供使用者參考。<br>**Codec** – 每個通訊埠的預設 Codec 設定都會顯示在本區，您可以按索引號碼變更每個電話通訊埠的設定。<br>**音調** – 顯示進階頁面所設定的音調值。<br>**音量** - 顯示進階頁面中 Mic/Speaker 的音量設定。<br>**預設 SIP 帳號** – “draytel_1” 是預設的 SIP 帳號，您可按索引下方的編號變更 SIP 帳號設定。<br>**DTMF Relay** –顯示進階頁面中所設定的 DTMF 模式。 |
| **RTP** | **Symmetric RTP** – 勾選此方塊啓用此功能。若要讓資料傳輸能在本機路由器與遠端路由器之間暢行無阻而不至於因 IP 漏失而誤導的情形發生，請您勾選此方塊解決這個問題。<br>**RTP 通訊埠起點** - 指定 RTP 之通訊埠起點，預設值爲 10050。<br>**RTP 通訊埠終點** - 指定 RTP 之通訊埠終點，預設值爲 15000。<br>**RTP TOS** –此項可決定 VoIP 封包的等級，請使用下拉式選項選擇其中一種。 |

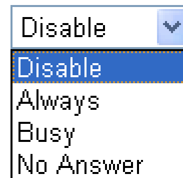



## Phone Port 細節設定

請按索引欄位下方的 1 或 2 連結進入設定頁面。

| | |
|---|---|
| **熱線** | 勾選此方塊啓用此功能，請在本區輸入 SIP URL 讓系統在您拿起話機後自動撥號。 |
| **連線計數器** | 勾選此方塊啓用此功能，您在本區所設定的限制時間內如果沒有任何回應，連線電話將會自動關閉。 |
| **指定轉接** | 共有四種選項可以選擇，**停用**可關閉此功能，**永遠**則表示來電會一直轉接到 SIP URL 上，**忙線**則表示來電只在本機忙碌 |

時轉接到 SIP URL，**沒回應**則表示來電若未收到任何回應，電話都會在切斷時轉接到 SIP URL 上。




**SIP URL** – 請輸入 SIP URL (例如 aaa@draytel.org 或 abc@iptel.org) 做為轉送電話的終點。

**逾時** – 設定電話轉接的逾時現制，預設值為 30 秒。

**DND (勿干擾)**

設定一段和平時間不受任何 VoIP 來電的干擾。在此期間，撥號進來的人會聽到忙線的聲音，而本機用戶則聽不到任何電話鈴聲。

**索引(1-60) 於電話簿** - 輸入例外電話於此方塊內，列於此之電話不受勿干擾的限制。詳細設定請參考**電話簿**一節。

**話中插接**

勾選此方塊啓用此功能，提示聲音將會出現以告知使用者有電話在等待。

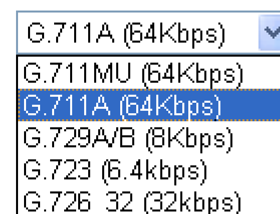
**電話轉接**

勾選此方塊啓用此功能，按轉接鍵轉接另一通電話，當電話連線成功時，掛上電話。此時另外二方就可直接溝通。

**偏好 Codec**

有五種不同的 CODEC 供您選擇，但真正被使用的 CODEC 在通訊建立前是和對方共同商議而得。預設的 CODEC 是 G.729A/B，它佔據較少的頻寬但是卻仍擁有良好的聲音品質，如果您想要使用 G.711，您最好具有至少 256Kbps 的上傳速率。

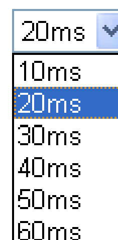
Prefer Codec




**單一 Codec** - 如果勾選此方塊，只有選定的 Codec 會被路由器套用。

**語音資料長度** - 資料總數包含單一封包(10, 20, 30, 40, 50 和 60)，預設值為 20ms，表示資料封包含 20ms 聲音資訊。

Packet Size




**語音活動偵測器(AVD)** - 選擇**開啓**啓動此項功能，以檢測使用者是否正在交談。如果安靜無聲，路由器將採取行動節省

頻寬的使用。

Voice Active Detector | Off
Off
On

**預設 SIP 帳號** 您可以設定 SIP 帳號(最多 6 組)，請使用下拉式清單選擇其中一組作爲預設帳號。
**當帳號已經註冊時請使用撥號音** - 勾選此方塊啓用此功能。

此外，您也可以按**進階**按鈕進入深一層的設定。此項設定是爲了符合路由器安裝所在地區的電信習慣而提供，錯誤音調設定可能會造成使用者的不便。關於設定話機的聲音型態，方法很簡單，只要選擇適當的區域讓系統自動尋找事先設定的音調設定和呼叫 ID 類型，或是您也可選擇使用者自訂，然後以手動方式調整音調，TOn1, TOff1, TOn2 和 TOff2 表示音調型態的韻律，TOn1 和 TOn2 表示開啓聲音；TOff1 和 TOff2 則表示關閉聲音。

VoIP >> Phone Settings

Advance Settings >> Phone1

Tone Settings

Region: User Defined — Caller ID Type: FSK_ETSI

| | Low Freq (Hz) | High Freq (Hz) | T on 1 (msec) | T off 1 (msec) | T on 2 (msec) | T off 2 (msec) |
|---|---|---|---|---|---|---|
| Dial tone | 350 | 440 | 0 | 0 | 0 | 0 |
| Ringing tone | 400 | 450 | 400 | 200 | 400 | 2000 |
| Busy tone | 400 | 0 | 375 | 375 | 0 | 0 |
| Congestion tone | 0 | 0 | 0 | 0 | 0 | 0 |

Volume Gain

Mic Gain(1-10): 5

Speaker Gain(1-10): 5

DTMF

DTMF Mode: InBand

Payload Type(RFC2833): 101

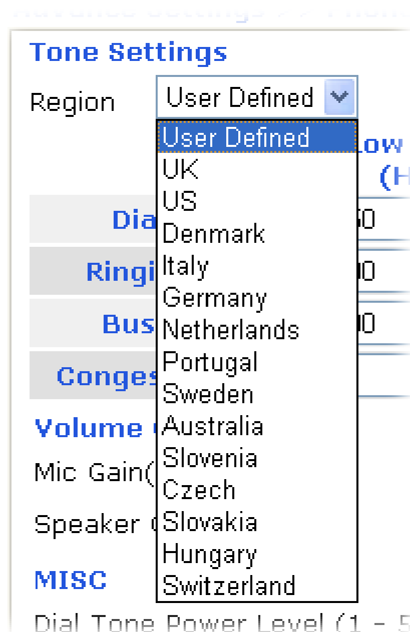
MISC

Dial Tone Power Level (1 - 50): 27

Ring Frequency (10 - 50HZ): 25

OK Cancel

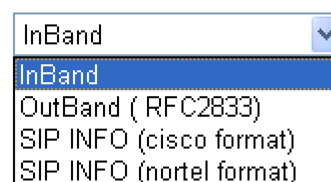
**Region** 選擇您目前所處地區，**來電顯示類型**、**撥號音**、**響鈴音**、**忙線音**和**系統擁塞音**都會自動顯示在本頁面上。如果您無法找到適合的地區，請您選擇**使用者自訂**，再自行輸入頁面所需的各式資料。




您也可以是個人需要指定各個區域內容，建議您採用預設值作為 VoIP 通訊之用。

| | |
|---|---|
| **來電顯示類型** | 此處提供數種標準，以便在電話機面板上顯示來電者的身分，請依照路由器安裝所在地區選擇適合的類型，如果您不知道話機究竟支援哪種標準，請直接採用預設值。 |
| **音量控制** | 請輸入 1- 10 以設定麥克風的音量，數字越大聲音越大。 |
| **雜項** | **撥號音量控制** -此項設定用來調整撥號的音量大小，數字越小音量越大，建議使用預設值。<br>**振鈴聲頻率** 此項設定用來驅動鈴聲的頻率，建議使用預設值。 |
| **DTMF** | **DTMF 模式**<br>***InBand -*** 當您按壓電話上的鍵盤時，路由器將會直接以聲音模式傳送 DTMF 音調。<br>***OutBand -*** 路由器將會抓取您所按壓的鍵盤號碼然後以數位格式傳送至另一端；接收者將會依照所接收的數位格式來產生音調。這個功能在網路擁塞的情形下是很有用處的，因為它仍可保持 DTMF 音調的準確度。<br>***SIP 資訊***路由器將抓取 DTMF 音調然後以 SIP 訊息轉送給遠端用戶。 |

DTMF mode




**Payload 類型 (rfc2833)** - 請自 96 至 127 中選擇一個數字，預設值為 101，此項設定只對 OutBand (RFC2833)模式有效。

## 3.5.4 狀態

在 VoIP 撥號狀態下，您可以看見 VoIP 1 和 VoIP 2 的 codec、連線情形和其他重要的撥號狀態資料。

VoIP >> Status

Status　　Refresh Seconds: 10 　Refresh

| Port | Status | Codec | PeerID | Elapse (hh:mm:ss) | Tx Pkts | Rx Pkts | Rx Losts | Rx Jitter (ms) | In Calls | Out Calls | Miss Calls | Speaker Gain |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phone1 | IDLE | | | 00:00:00 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 5 |
| Phone2 | IDLE | | | 00:00:00 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 5 |

Log

| Date (mm-dd-yyyy) | Time (hh:mm:ss) | Duration (hh:mm:ss) | In/Out/Miss | Account ID | Peer ID |
|---|---|---|---|---|---|
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |

**更新間隔秒數**　指定更新的間隔秒數以取得最新的 VoIP 撥號資訊，當按下**更新頁面**按鈕時，頁面資訊將會立即更新。

Refresh Seconds : 10
5
10
30

**通訊埠**　顯示目前 VoIP 電話的連線通訊埠(Phone1 / Phone2)。

**狀態**　顯示 VoIP 連線狀態。
**IDLE -**表示 VoIP 功能正處於閒置狀態。
**HANG_UP -**表示連線並未建立(忙線音調)。
**CONNECTING -**表示用戶正撥出號碼中。
**WAIT_ANS -**表示已連線並等待遠端用戶的回答。
**ALERTING -**表示有來電。
**ACTIVE-**表示 VoIP 連線啓動。

**Codec**　表示目前頻道所利用的聲音 codec。

**對方 ID**　撥進或撥出之對方 ID (格式可以是 IP 位址或是網域名稱)。

**經過時間**　通話時間以秒數計算。

**傳送封包數**　在連線中全部的傳送封包數量。

**接收封包數**　在連線中全部的接收封包數量。

**漏失接收封包**　在連線中漏失的全部封包。

**接收抖動**　接收聲音封包抖動狀態。

**來電**　已接來電總數。

**撥出電話**　撥出電話總數。

**接聽音量**　電話音量大小。

**記錄** 顯示 VoIP 電話紀錄。

## 3.6 無線區域網路設定

本節所提供的資訊僅針對 *n* 系列機型。

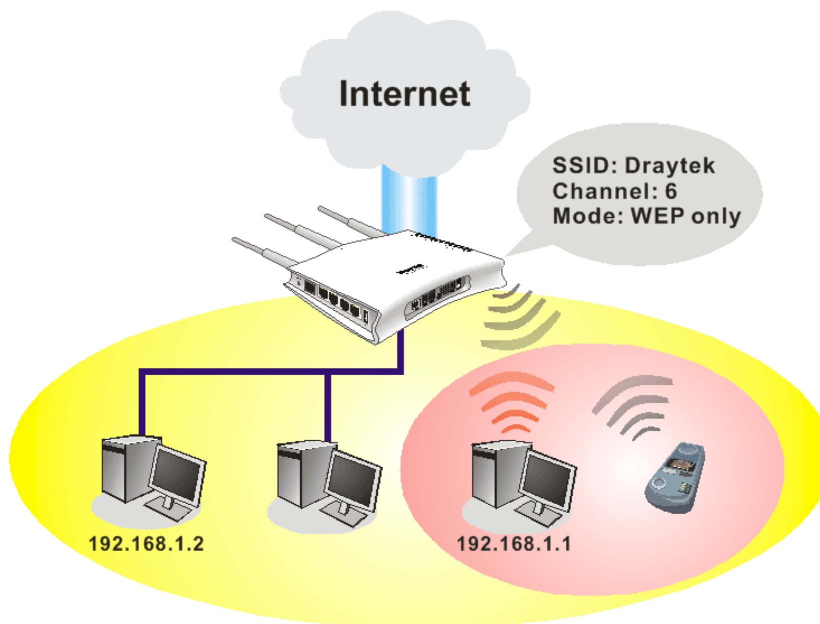
### 3.6.1 基本觀念

在最近幾年無線通訊的市場有了極大的成長，無線技術線在到達了或說是有能力到達地球表面上的每一個點，數以百萬的人們每天透過無線通訊產品彼此交換資訊，Vigor G 系列路由器，又稱爲 Vigor 無線路由器，被設計成爲一個適合小型辦公室/家庭需要的路由器，擁有最大的彈性與效率，任何一個被授權的人，都可以攜帶內建的無線區域網路用戶端 PDA 或是筆記型電腦，進入會議室開會，因而不需擺放一堆亂七八糟的纜線或是到處鑽孔以便連線。無線區域網路機動性高，因此無線區域網路使用者可以同時存取所有區域網路中的工具，以及遨遊網際網路，好比是以有線網路連接的一樣。

Vigor 無線路由器皆配有與標準 IEEE 802.11n draft 2 通訊協定相容之無線區域網路介面，爲了進一步提高其效能，Vigor 路由器也承載了進階無線技術以便將速率提升至 300 Mbps*，因此在最後您可以非常順利的享受流暢的音樂與影像。

| **注意**：*資料的實際總處理能力會依照網路條件和環境因素而改變，如網路流量、網路費用以及建造材料。 |
|---|

在無線網路的基礎建設模式(Infrastructure Mode)中，Vigor 無線路由器扮演著無線網路基地台(AP)的角色，可連接很多的無線用戶端或是無線用戶站(STA)，所有的用戶站透過路由器，都可分享相同的網際網路連線。**基本設定**可讓您針對無線網路所需的訊息包含 SSID、頻道等項目做基本的配置。




**安全防護概要**

**即時硬體加密:** Vigor 路由器配有 AES 加密引擎，因此可以採用最高級的保護措施，在不影響使用者的習慣之下，對資料達成保護效果。

**完整的安全性標準選項:** 爲了確保無線通訊的安全性與私密性，提供數種市場上常見的無線安全標準。

有線對應隱私權(Wired Equivalent Privacy, WEP)是一種傳統的方法，使用 64-bit 或是 128-bit 金鑰透過無線收發裝置來加密每個資料訊框。通常無線基地台會事先配置一組含四個金鑰的設定，然後使用其中一個金鑰與每個無線用戶端通訊聯絡。

Wi-Fi 保護存取協定(Wi-Fi Protected Access, WPA)是工業上最佔優勢的安全機制，可分成二大類：WPA-personal 或稱為 WPA Pre-Share Key (WPA/PSK)以及 WPA-Enterprise 又稱為 WPA/802.1x。

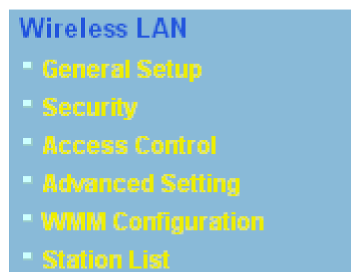
在 WPA-Personal 機制中，會應用一個事先定義的金鑰來加密傳輸中的資料，WPA 採用 Temporal Key Integrity Protocol (TKIP) 加密資料而 WPA2 則是採用 AES，WPA-Enterprise 不只結合加密也還涵括驗證功能。

由於 WEP 已被證明是有弱點的，您可以考慮使用 WPA 作為安全連線之用。您應該按照所需來選擇適當的安全機制，不論您選擇哪一種安全防護措施，它們都可以全方位的加強您無線網路上之資料保護以及/或是機密性。Vigor 無線路由器是相當具有彈性的，且能同時以 WEP 和 WPA 支援多種安全連線。

**分隔無線與有線區域網路 - 無線區域網路隔離**可使您自有線區域網路中，分隔出無線區域網路以便隔離或是限制存取。隔離代表著雙方彼此都無法存取對方的資料，欲詳細說明商業用途之範例，您可以為訪客設定一個無線區域網路，讓他們只能連接到網際網路而不必擔心洩露機密資訊。更彈性的作法是，您可以新增 MAC 位址的過濾器來區隔有線網路之單一使用者的存取行為。

**管理無線用戶端 - 無線用戶端列表**顯示無線網路中全部的無線用戶端以及連接狀態。

以下為**無線區域網路**下的功能項目：




## 3.6.2 基本設定

按下**一般設定**連結，新的網頁即會開啓，您可以設定 SSID 和無線頻道資訊，請參考下圖：

Wireless LAN >> General Setup

General Setting ( IEEE 802.11 )

☑ Enable Wireless LAN

Mode : Mixed(11b+11g+11n)

Index(1-15) in Schedule Setup: ___, ___, ___, ___

Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored.

SSID: DrayTek

Channel : Channel 6, 2437MHz

Packet-OVERDRIVE™

☐ Tx Burst

Note:

The same technology must also be supported in clients to boost WLAN performance.

☐ Hide SSID

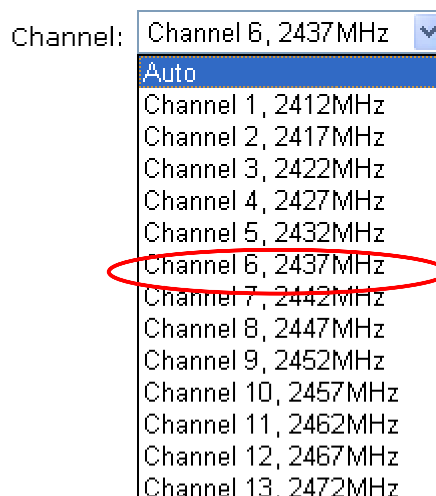
☐ Long Preamble

Hide SSID: prevent SSID from being scanned.

Long Preamble: necessary for some older 802.11b devices only (lowers performance).

OK Cancel

| | |
|---|---|
| **啓用** | 勾選此方塊啓動無線功能。 |
| **模式** | 請選擇一個適當的無線模式。目前路由器支援的協定有綜合( (11b+11g), 11g Only, 11b Only, 綜合( (11g+11n), 11n Only 及綜合( (11b+11g+11n)。 請選擇綜合 (11b+11g+11n) 模式。<br>Mixed(11b+11g+11n)<br>11b Only<br>11g Only<br>11n Only<br>Mixed(11b+11g)<br>Mixed(11g+11n)<br>Mixed(11b+11g+11n) |
| **SSID** | 預設的 SSID 值爲 **DrayTek** 建議您變更爲另一個特殊名稱。它是無線區域網路的身分辨識碼，SSID 可以是任何文字、數字或是各種特殊字元。 |
| **道** | 無線區域網路的通道頻率，預設頻道是 6，如果選定的頻道受到嚴重的干擾的話，您可自行切換爲其他頻道。如果您不知道該選何種通道頻率的話，請選擇**自動**即可。 |




| | |
|---|---|
| **隱藏 SSID** | 勾選此方塊，防止他人得知 SSID 值，未知此路由器的 SSID 之無線用戶在搜尋網路時，看不到 Vigor 無線路由器的訊息。 |
| **長封包標頭** | 此選項用來定義 802.11 封包中同步區塊的長度，最新的無線網路以 56 bit 同步區來使用短封包標頭，而不是以 128 bit 同步區來使用長封包標頭。不過，一些原始 11b 無線網路裝置只有支援長封包標頭而已，因此如果您需要和此種裝置通訊溝通的話，請勾選此方塊。 |

## 3.6.3 安全性設定

擇**安全性設定**後，新的網頁將會出現，您可以在此頁面上調整 WEP 和 WPA 設定。

Wireless LAN >> Security Settings

Security Settings

Mode: Disable

WPA:

Encryption Mode: TKIP

Pre-Shared Key(PSK): **************

Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".

WEP:

Encryption Mode: 64-Bit

Key 1 : **************

Key 2 : **************

Key 3 : **************

Key 4 : **************

For 64 bit WEP key
Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132".

For 128 bit WEP key
Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "0123456789abc" or "0x30313233343536373839414243".

OK Cancel

**模式** 此一設定有數種模式可供您選擇。

Mode: Disable
Disable
WEP
WPA/PSK
WPA2/PSK
Mixed(WPA+WPA2)/PSK

**停用** - 關閉加密機制。
**WEP -** 只接受 WEP 用戶以及僅接受以 WEP 金鑰輸入的加密鑰匙。
**WPA/PSK -**接受 WPA 用戶，請在 PSK 中輸入加密金鑰。
**WPA2/PSK -**接受 WPA2 用戶，請在 PSK 中輸入加密金鑰。
**綜合 (WPA+ WPA2)/PSK –** 同時接受 WPA 與 WPA2 用戶，請在 PSK 中輸入加密金鑰。

**WPA** WPA 可藉由金鑰加密每個來自無線網路的訊框，可在本區手動輸入 PSK，或是藉由 802.1x 驗證方式來自動加密。
**類型** – 選擇綜合 (WPA+WPA2) 或 WPA2。
**預先共用金鑰 (PSK)** - 輸入 **8~63** 個 ASCII 字元，像是 012345678（或是 64 個 16 進位數字，以 0x 開頭，如 0x321253abcde...）。

**WEP** **64-Bit** - 針對 64 位元的 WEP 金鑰，請輸入 5 個 ASCII 字元，像是 12345（或是 10 個 16 進位數字，以 0x 開頭，如 0x4142434445）。

**128-Bit** - 針對128位元的WEP金鑰，請輸入13個ASCII字元，像是 ABCDEFGHIJKLM（或是 16 個 16 進位數字，以 0x 開頭，如 0x4142434445）。

Encryption Mode: 64-Bit / 64-Bit / 128-Bit

所有的無線裝置都必須支援相同的 WEP 加密位元大小，並擁有相同的金鑰。這裡可以輸入四組金鑰，但一次只能選擇一組號碼來使用，這些金鑰可以 ASCII 文字或是 16 進位字元來輸入。請點選您想使用的金鑰組別。

### 3.6.4 連線控制

爲了增加額外的無線存取安全性，連線控制頁面可讓您透過無線區域網路的用戶 MAC 位址來限制網路存取動作。只有設定有效的 MAC 位址得以存取無線區域網路介面，請選**連線控制**連結，開啓新的網頁，如同下圖所示，您即可在此頁面上編輯用戶端的 MAC 位址達到控制其存取權的目的。

Wireless LAN >> Access Control

Access Control

☑ Enable Access Control

Policy : Activate MAC address filter

MAC Address Filter

Index Attribute MAC Address

Client's MAC Address : __ : __ : __ : __ : __ : __

Attribute :

☐ s: Isolate the station from LAN

Add Delete Edit Cancel

OK Clear All

| | |
|---|---|
| **啓用連線控制** | 勾選此項以啓動 MAC 位址存取控制作用。 |
| **規則** | 選擇一項規則，請挑選**啓用 MAC 位址過濾程式**以便在下方手動輸入其他用戶的 MAC 位址；挑選**隔離無線網路和有線網路**可以 MAC 位址清單爲基礎，自區域網路中隔開所有的無線網路用戶站。 |
| **MAC 位址過濾** | 顯示之前編輯的全部 MAC 位址。 |
| **客戶端的 MAC 位址** | 請手動輸入無線用戶端的 MAC 位址。 |
| **特性** | **s -**勾選此項以便隔離無線用戶端之無線連線。 |
| **新增** | 新增新的 MAC 位址於清單上。 |
| **刪除** | 刪除清單中選定的 MAC 位址。 |

| | |
|---|---|
| **編輯** | 編輯清單中選定的 MAC 位址。 |
| **取消** | 放棄連線控制設定。 |
| **確定** | 按此鈕儲存連線控制清單。 |
| **全部清除** | 按此鈕儲存連線控制清單。 |

### 3.6.7 無線用戶端列表

**無線用戶端列表**提供您目前相連之無線用戶的狀態碼，下圖針對狀態碼提供了詳盡的解說，為了能有更方便的連線控制，您可以選擇一台 WLAN 用戶站然後選擇**新增到連線控制**，這樣就可以了。

Wireless LAN >> Station List

Station List

Status MAC Address Associated with

Refresh

Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.

Note: After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.

Add to Access Control :

Client's MAC address : : : : :

Add

| | |
|---|---|
| **更新頁面** | 按此鈕更新用戶端的 MAC 位址列表。 |
| **新增** | 按此鈕新增選定之 MAC 位址至**連線控制**。 |

## 3.7 系統維護

系統設定方面，有數種項目是使用者需要了解的：系統狀態、使用者密碼、時間設定、重啓系統等等。

下圖為系統維護的主要設定功能。

| System Maintenance |
|---|
| System Status |
| User Password |
| Time and Date |
| Reboot System |

### 3.7.1 系統狀態

系統狀態提供基本的網路設定，包含區域網路和 WAN 介面等資訊，同時您也可以獲得目前執行中的韌體版本或是韌體其他的相關資訊。

**System Status**

| | |
|---|---|
| Model Name | : Vigor2110 series |
| Firmware Version | : 3.3.0_RC5 |
| Build Date/Time | : Feb 11 2009 14:25:46 |

| LAN | |
|---|---|
| MAC Address | : 00-50-7F-9A-32-70 |
| 1st IP Address | : 192.168.1.5 |
| 1st Subnet Mask | : 255.255.255.0 |
| DHCP Server | : Yes |
| DNS | : 172.16.3.18 |

| WAN | |
|---|---|
| Link Status | : Connected |
| MAC Address | : 00-50-7F-9A-32-71 |
| Connection | : DHCP Client |
| IP Address | : 192.168.5.26 |
| Default Gateway | : 192.168.5.1 |

| VoIP | | | |
|---|---|---|---|
| Port | Profile | Reg. | In/Out |
| Phone1 | | No | 0/0 |
| Phone2 | | No | 0/0 |

| Wireless LAN | |
|---|---|
| MAC Address | : 00-50-7f-9a-32-70 |
| Frequency Domain | : Europe |
| Firmware Version | : 1.8.1.0 |
| SSID | : DrayTek |

| | |
|---|---|
| **型號名稱** | 顯示路由器的型號名稱。 |
| **韌體版本** | 顯示路由器的韌體版本。 |
| **建立日期與時間** | 顯示目前韌體建立的日期與時間。 |
| ***LAN-------*** | |
| **MAC 位址** | 顯示區域網路介面的 MAC 位址。 |
| **第一個 IP 位址** | 顯示區域網路介面的 IP 位址。 |
| **第一個子網路遮罩** | 顯示區域網路介面的子網路遮罩位址。 |
| **DHCP 伺服器** | 顯示區域網路介面的 DHCP 伺服器目前的狀態。 |
| **DNS** | 顯示主要 DNS 的 IP 位址。 |
| ***WAN-------*** | |
| **連線狀態** | 顯示目前的實體連線狀況。 |
| **MAC 位址** | 顯示 WAN 介面的 MAC 位址。 |
| **IP 位址** | 顯示 WAN 介面的 IP 位址。 |
| **預設閘道** | 顯示預設閘道指定的 IP 位址。 |
| ***Wireless LAN-------*** | |
| **MAC 位址** | 顯示無線區域網路的 MAC 位址。 |
| **頻率網域** | 網域可以是歐洲(13 個可用頻道),美國(11 個可用頻道)，無線產品所支援之可用頻道在不同的國家下是不相同的。 |

**韌體版本** 表示配備 WLAN miniPCi 卡的詳細資訊，同時可以提供該卡相關的特徵訊息。

**SSID** 顯示路由器的 SSID 。

## 3.7.2 使用者密碼

本頁允許您設定新的密碼。

System Maintenance >> User Password

User Password

| | |
|---|---|
| Old Password | |
| New Password | |
| Confirm Password | |

OK

**舊密碼** 請輸入舊密碼，出廠預設值是空白的。

**新密碼** 請在本區輸入新密碼。

**確認密碼** 再次輸入新密碼以確認。

當您按下**確定**鍵後，登入視窗將會出現，請使用新的密碼以便再次存取網頁設定頁面。

## 3.7.3 時間和日期

允許您指定自何處取得路由器時間。

System Maintenance >> Time and Date

Time Information

| | | |
|---|---|---|
| Current System Time | 2009 Mar 27 Fri 8 : 32 : 8 | Inquire Time |

Time Setup

- ○ Use Browser Time
- ◉ Use Internet Time Client

| | |
|---|---|
| Server IP Address | pool.ntp.org |
| Time Zone | (GMT) Greenwich Mean Time : Dublin |
| Enable Daylight Saving | ☐ |
| Automatically Update Interval | 30 min |

OK Cancel

**C 目前系統時間** 按**取得時間**按鈕取得目前時間。

**使用本台 PC 的時間** 選擇此項以便採用遠端管理者電腦上的瀏覽器時間，作。

**使用網際網路的時間伺服器** 選擇此項以便自網際網路上的時間伺服器選擇所需的時間資訊。

**時間協定** 選擇適合本地的時間協定。

**伺服器 IP 位址** 輸入時間伺服器的 IP 地址。

**時區** 選擇路由器所在的時區。

**自動更新間隔** 選定時間間隔以供 NTP 伺服器更新之用。

全部設定完成之後請按**確定**儲存目前的設定。

### 3.7.4 重啓路由器

網路設定可以用來重新啓動路由器，請自**系統維護**中按**重啓路由器**開啓如下頁面。

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

Using current configuration

OK

如果您想要使用目前的設定來重新啓動路由器，請勾選**使用目前組態**，然後按**確定**；如果要重設路由器設定回復成爲預設值，請勾選**使用原廠預設組態**，然後按**確定**，路由器將會花 5 秒重新啓動系統。

**注意:**.當系統在您完成網頁設定並跳出**重啓路由器**網頁後，請務必按下**確定**以重新啓動路由器，這個動作可以確保系統的操作正常，且可避免未來發生不預期的錯誤。

## 3.8 我診斷工具

自我診斷工具提供一個非常有效的方式，讓使用者能夠檢視或是診斷路由器的現況。以下為自我診斷的選單項目：




### 3.8.1 DHCP 表

此工具提供指派 IP 位址的相關資訊，這項資訊對於診斷網路問題像是 IP 位址衝突等是很有幫助的。

按**自我診斷工具**，選擇 **DHCP 表**開啓相關網頁。

Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table | Refresh |

```
DHCP server: Running
Index   IP Address      MAC Address             Leased Time     HOST ID
1       192.168.1.12    00-1D-4F-D5-C1-39       4:16:43.820     iPod-3
```

| | |
|---|---|
| **Index** | 顯示連線項目編號。 |
| **IP Address** | 顯示路由器指派給特定電腦的 IP 位址。 |
| **MAC Address** | 顯示 DHCP 指派給特定電腦的 MAC 位址。 |
| **Leased Time** | 顯示指定電腦的租約時間。 |
| **HOST ID** | 顯示指定電腦的主機 ID 名稱。 |
| **更新頁面** | 按此鈕重新載入本頁。 |

## 3.8.2 Ping 自我診斷

按**自我診斷工具**，選擇 **Ping 自我診斷**開啓相關網頁。

Diagnostics >> Ping Diagnosis

Ping Diagnosis

Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".

Ping to: Host / IP    IP Address:

Run

Result | Clear |

**Ping 至** 使用下拉式清單選擇您想要 Ping 的目標。

**IP 位址** 輸入您想要 Ping 的主機/IP 上的 IP 位址。

**執行** 按此鈕啓動 Ping 作業，結果將會顯示在螢幕上。

**清除** 按此連結清除視窗上的結果。

## 3.8.3 追蹤路由

按下**診斷工具**，選擇**追蹤路由**開啓相關網頁。本頁允許您追蹤路由器至主機之間的路由情況，只要簡單的輸入主機的 IP 位址並按下執行按鈕，整個路由狀況都將顯示在螢幕上。

Diagnostics >> Trace Route

Trace Route

Protocol: ICMP

Host / IP Address:    Run

Result | Clear |

**追蹤經由介面** 使用下拉式清單選擇您想要經由其處來追蹤的 WAN 介面，或使用**不指定**讓路由器自動決定選擇哪一種介面。

**主機/IP 位址** 指明主機的 IP 位址。

**執行** 按此鈕開始路由追蹤動作。

**清除** 按此連結刪除視窗上的結果。

# 4 管理者操作模式

## 4.1 網際網路連線控制

快速安裝精靈提供使用者一個簡單的方法，以便能快速設定路由器的連線模式。如果您想要針對不同廣域網路模式調整更多的設定，請前往 **WAN** 群組然後點選**網際網路連線控制**連結。本節將會為您介紹一些網際網路的基本觀念，並詳細說明所有的連線模式。

### 4.1.1 網路的基本概念

IP 表示網際網路通訊協定，在以 IP 為主的網路像是路由器、列印伺服器和主機電腦的每一種裝置，都需要一組 IP 位址作為網路上身分辨識之用。為了避免位址產生衝突，IP 位址都必須於網路資訊中心(NIC) 公開註冊，擁有個別 IP 位址對那些於真實網路分享的裝置是非常必要的，但在虛擬網路上像是路由器所掌管下的主機電腦就不是如此，因為它們不需要讓外人從真實地區進入存取資料。因此 NIC 保留一些永遠不被註冊的特定位址，這些被稱之為虛擬 IP 位址，範圍條列如下：

**從 10.0.0.0 到 10.255.255.255**
**從 172.16.0.0 到 172.31.255.255**
**從 192.168.0.0 到 192.168.255.255**

#### 什麼是真實 IP 位址和虛擬 IP 位址

由於路由器扮演著管理及保護其區域網路的角色，因此它可讓主機群間互相聯繫。每台主機都有虛擬 IP 位址，是由路由器的 DHCP 伺服器所指派，路由器本身也會使用預設之虛擬 IP 位址 192.168.1.1 與本地主機達成聯繫目的，同時，Vigor 路由器可藉由真實 IP 位址與其他的網路裝置溝通連接。當資料經過時，路由器的網路位址轉換(NAT)功能將會在真實與虛擬位址間執行轉換動作，封包將可傳送至本地網路中正確的主機電腦上，如此一來，所有的主機電腦就都可以共享一個共同的網際網路連線。

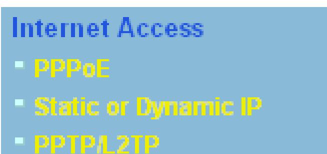
#### 取得 ISP 提供的真實 IP 位址

欲取得 ISP 提供的真實 IP 位址，以便將路由器當成用戶假定之設備，有幾種種常見的模式可以選用：**Point to Point Protocol over Ethernet (PPPoE),** 和 **MPoA**.等，**Multi-PVC** 是提供給您執行更進階的設定。

在 ADSL 之部署中，PPP (Point to Point)型態之驗證和授權是橋接用戶前端設備所需要的。PPPoE (Point to Point Protocol over Ethernet )透過一台存取裝置連接網路主機至遠端存取集中器，此種應用讓使用者覺得操作路由器是很簡單的，同時也可依照使用者的需要提供存取控制及服務類型。

當路由器開始連接至 ISP 時，路由器將執行一系列過程以尋求連線，然後即可產生一個 session，您的使用者辨識名稱和密碼由 **RADIUS** 驗證系統的 **PAP** 或 **CHAP** 來驗證，通常您的 IP 位址、DNS 伺服器和其他相關資訊都是由 ISP 指派的。

下圖為 WAN 的功能項目：




## 4.1.2 PPPoE

如果想要使用 PPPoE 作爲網際網路連線的通訊協定，請自 **Internet Access** 功能項目中選擇 **PPPoE** 模式，下面的設定網頁將會出現。

Internet Access >> PPPoE

PPPoE Client Mode

| PPPoE Setup | PPP/MP Setup |
|---|---|
| PPPoE Link ○ Enable ⦿ Disable | PPP Authentication [PAP or CHAP] |
| ISP Access Setup | ☑ Always On |
| Username [ ] | Idle Timeout [-1] second(s) |
| Password [ ] | IP Address Assignment Method (IPCP) [WAN IP Alias] |
| Index(1-15) in Schedule Setup: => [ ], [ ], [ ], [ ] | Fixed IP ○ Yes ⦿ No (Dynamic IP) |
| | Fixed IP Address [ ] |
| WAN Connection Detection | ⦿ Default MAC Address |
| Mode [ARP Detect] | ○ Specify a MAC Address |
| Ping IP [ ] | MAC Address: |
| TTL: | 00 . 50 . 7F : 9A . 32 . 71 |

OK

**PPPoE 用戶端模式** 按下**啓用**按鈕可啓動此功能，如果您選的是**停用**，此項功能將會關閉，全部調整過的設定也都將立即失效。

**ISP 存取設定** 輸入使用者名稱、密碼和驗證參數，按照 ISP 所提供給您的訊息。
**使用者名稱** –在本區請輸入 ISP 提供的使用者名稱。
**密碼** – 在本區請輸入 ISP 提供的密碼。
**索引號碼(1-15) 於排程設定** -可以輸入四組時間排程，全部的排程都是在**應用-排程**網頁中事先設定完畢，您可在此輸入該排程的索引編號。

**WAN 連線檢測** 這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。
模式 – 選擇 **ARP Detect 或 Ping Detect** 執行 WAN 檢測動作。
**Ping IP** – 如果您選擇 **Ping Detect** 作爲檢測模式，您必須在本區輸入 IP 位址作爲 Ping 檢測之用。
**TTL (Time to Live)** – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。

**PPP/MP 設定** **PPP 驗證** – 選擇 **PAP** 或是 **PAP 或 CHAP**。
**閒置逾時** – 設定網際網路在經過一段沒有任何動作的時間後自

動斷線的時間，此項設定只在 **WAN>>一般設定**網頁中的**啓動模式**選擇了**需求時連線**才會有作用

**IP 位址指派方式 (IPCP)**

通常每次的連線，ISP 會隨機指派 IP 位址給您，在某些情況下，您的 ISP 可以提供給您相同的 IP 位址，不論您何時提出要求。您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。

**WAN IP 別名** - 如果您有數個真實 IP 位址且想要在 WAN 介面上使用，請使用此功能。除了目前使用的這一組之外，您還可以設定多達 8 組的真實 IP 位址。

http://192.168.1.5 - WAN IP Alias - Microsoft Internet Explorer

WAN IP Alias ( Multi-NAT )

| Index | Enable | Aux. WAN IP | Join NAT IP Pool |
|---|---|---|---|
| 1. | v | 172.16.3.229 | v |
| 2. | ☐ | | ☐ |
| 3. | ☐ | | ☐ |
| 4. | ☐ | | ☐ |
| 5. | ☐ | | ☐ |
| 6. | ☐ | | ☐ |
| 7. | ☐ | | ☐ |
| 8. | ☐ | | ☐ |

OK Clear All Close

**固定 IP 位址** – 按**是**使用此功能並輸入一個固定的 IP 位址。
**預設 MAC 位址** – 您可以使用預設 MAC 位址或是在此區域中填入另一組位址。
**指定 MAC 位址** – 手動輸入路由器的 MAC 位址。

在您完成上述的設定之後，請按**確定**按鈕來啓動設定。

### 4.1.3 固定或動態 IP

對固定 IP 模式來說，通常您會收到 DSL 或是 ISP 服務供應商提供給您的一個固定的真實 IP 位址或是真實子網路，在大多數的情形下，Cable 服務供應商將會提供一個固定的真實 IP，而 DSL 服務供應商提供的是真實子網路資料。如果您有一組真實的子網路，您可以指派一組或是多組 IP 位址至 WAN 介面。

若要使用**固定或動態 IP** 爲網際網路的連線協定，請自 **WAN** 中選擇**網際網路連線**，接著選擇**固定或動態 IP**，即可出現下圖。

Internet Access >> Static or Dynamic IP

Static or Dynamic IP (DHCP Client)

Access Control
Broadband Access ◉ Enable ○ Disable

Keep WAN Connection
☐ Enable PING to keep alive
PING to the IP 0.0.0.0
PING Interval 0 minute(s)

WAN physical type
Auto negotiation

WAN Connection Detection
Mode ARP Detect
Ping IP
TTL:

RIP Protocol
☐ Enable RIP

WAN IP Network Settings [WAN IP Alias]
◉ Obtain an IP address automatically
Router Name *
Domain Name *
* : Required for some ISPs
○ Specify an IP address
IP Address 192.168.5.26
Subnet Mask 255.255.255.0
Gateway IP Address 192.168.5.1

◉ Default MAC Address
○ Specify a MAC Address
MAC Address:
00 . 50 . 7F : 9A . 32 . 71

DNS Server IP Address
Primary IP Address
Secondary IP Address

OK

**固定或動態 IP (DHCP 用戶端)** 按**啓用**以啓動此功能，如果您按的是**停用**，此功能將會關閉，您在此頁面所完成的全部設定都將失效。

**維持 WAN 連線** 正常情況下，這個功能是設計用來符合動態 IP 環境，因爲某些 ISP 會在一段時間沒有任何回應時中斷連線。請勾選**啓用 PING 以保持常態連線**。

**PING 到指定的 IP** – 如果您啓用此功能，請指定 IP 位址讓系統可以 PING 到該 IP 以保持連線

**PING 間隔** - 輸入間隔時間讓系統得以執行 PING 動作。

**WAN 連線檢測** 這個功能讓您檢查目前網路是否還在連線中。可透過 ARP 檢測或是 Ping Detect 來完成。

模式 – 選擇 **ARP Detect 或 Ping Detect** 執行 WAN 檢測動作。

**Ping IP** – 如果您選擇 **Ping Detect** 作爲檢測模式，您必須在本區輸入 IP 位址作爲 Ping 檢測之用。

**TTL (Time to Live)** – 顯示數值供您參考，TTL 數值是利用 Telnet 指令始可設定。

**RIP 協定** 指名路由器是如何變更路由表格資訊，勾選此項目以啓動此功能。

**WAN IP 網路設定** 這個區域允許您自動取得 IP 位址並讓您手動輸入 IP 位址。

**WAN IP 別名** - 如果您有多個真實 IP 位址，想要在 WAN 介面上利用這些 IP，請使用 WAN IP 別名。除了目前使用的 IP 外，您還可以另外設定 8 組真實 IP，要注意的是，本項設定僅針對 WAN1 有效用。

http://192.168.1.5 - WAN IP Alias - Microsoft Internet Explorer

WAN IP Alias ( Multi-NAT )

| Index | Enable | Aux. WAN IP | Join NAT IP Pool |
|---|---|---|---|
| 1. | v | 172.16.3.229 | v |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |
| 6. | | | |
| 7. | | | |
| 8. | | | |

OK　Clear All　Close

**自動取得 IP 位址** – 如果您想要使用**動態 IP** 模式，按此鈕以自動取得 IP 位址。

***路由器名稱***: 輸入 ISP 的路由器名稱。

***網域名稱***: 輸入指定的網域名稱。

**指定 IP 位址** – 按此鈕指定 IP 位址讓資料通過。

***IP 位址***:輸入 IP 位址。

***子網路遮罩***:輸入子網路遮罩。

***閘道 IP 位址***: 輸入閘道 IP 位址。

***預設 MAC 位址***: 按此鈕使用預設的 MAC 位址。

***指定 MAC 位址***: 部分 Cable 服務供應商會指定 MAC 位址作為存取驗證之用，此時您需要按下此鈕並在下方區域輸入 MAC 位址。

**DNS 伺服器 IP 位址** 若要使用固定 IP 模式，請輸入路由器的主要 IP 位址，如有必要，在將來，您也可以輸入次要 IP 位址以符合所需。

## 4.1.4 PPTP/L2TP

若要使用 **PPTP/L2TP** 為網際網路的連線協定，請自 **Internet Access** 中選擇 **PPTP/L2TP**，即可出現下圖。

Internet Access >> PPTP

PPTP Client Mode

| PPTP Setup | | PPP Setup | |
|---|---|---|---|
| PPTP Link | ○ Enable ⦿ Disable | PPP Authentication | PAP or CHAP |
| PPTP Server | | ☑ Always On | |
| **ISP Access Setup** | | Idle Timeout | -1 second(s) |
| Username | 123 | **IP Address Assignment Method (IPCP)** | |
| Password | ●●● | Fixed IP | ○ Yes ⦿ No (Dynamic IP) |
| Index(1-15) in Schedule Setup: | | Fixed IP Address | |
| => , , , | | **WAN IP Network Settings** | |
| | | ○ Obtain an IP address automatically | |
| | | ⦿ Specify an IP address | |
| | | IP Address | 172.16.3.229 |
| | | Subnet Mask | 255.255.0.0 |

OK

**PPTP Setup**

按**啓用**以啓動此功能，如果您按的是**停用**，此功能將會關閉，您在此頁面所完成的全部設定都將失效。

**PPTP Server** – 如果您啓用了 PPTP/L2TP 模式，請指定伺服器的 IP 位址。

**ISP 存取設定**

**使用者名稱** –在本區請輸入 ISP 提供的使用者名稱。

**密碼** – 在本區請輸入 ISP 提供的密碼。

**索引號碼(1-15) 於排程設定** -可以輸入四組時間排程，全部的排程都是在**應用-排程**網頁中事先設定完畢，您可在此輸入該排程的索引編號。

**PPP Setup**

**PPP Authentication** - Select **PAP only** or **PAP or CHAP** for PPP.

**Idle Timeout** - Set the timeout for breaking down the Internet after passing through the time without any action.

**IP 位址指派方式 (IPCP)**

通常每次的連線，ISP 會隨機指派 IP 位址給您，在某些情況下，您的 ISP 可以提供給您相同的 IP 位址，不論您何時提出要求。您只要在固定 IP 位址欄位中輸入 IP 位址就可以達成上述的目的。詳情請聯絡您的 ISP 業者。

**固定 IP 位址** –請輸入一組固定 IP。

**WAN IP 網路設定**

**自動取得 IP 位址** – 如果您想要使用**動態 IP** 模式，按此鈕以自動取得 IP 位址。

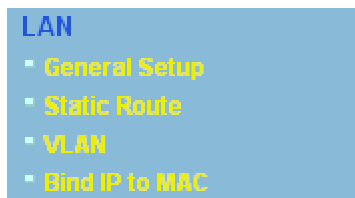
**指定 IP 位址** – 按此鈕指定 IP 位址讓資料通過。

***IP 位址:***輸入 IP 位址。

***子網路遮罩:***輸入子網路遮罩。

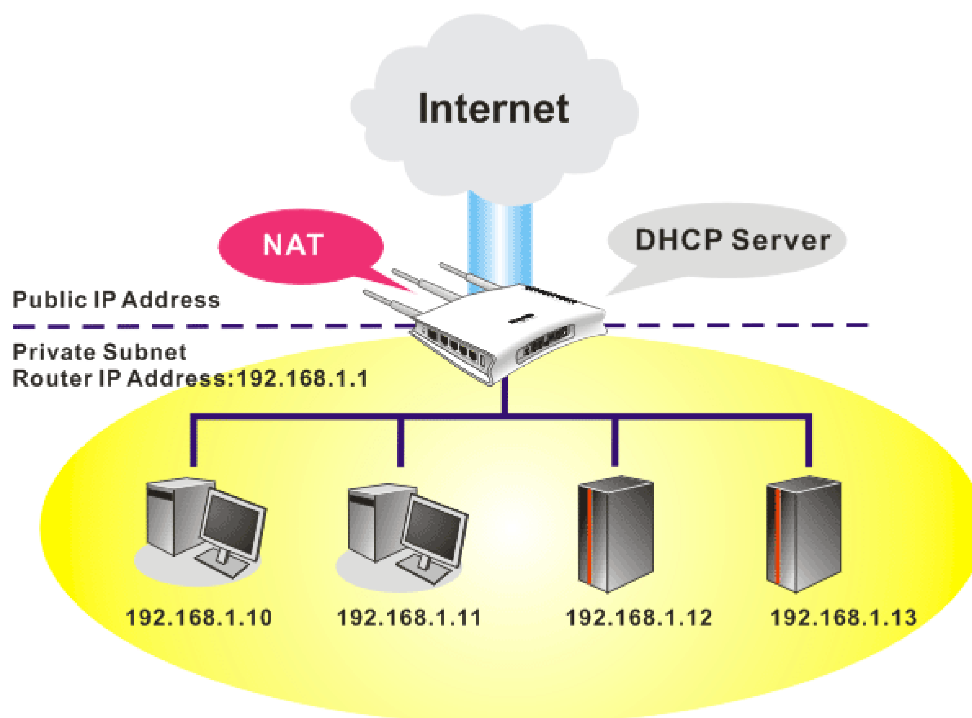
## 4.2 區域網路

區域網路是由路由器所管理的一群子網路，網路結構設計和您自 ISP 所取得之真實 IP 位址有關。

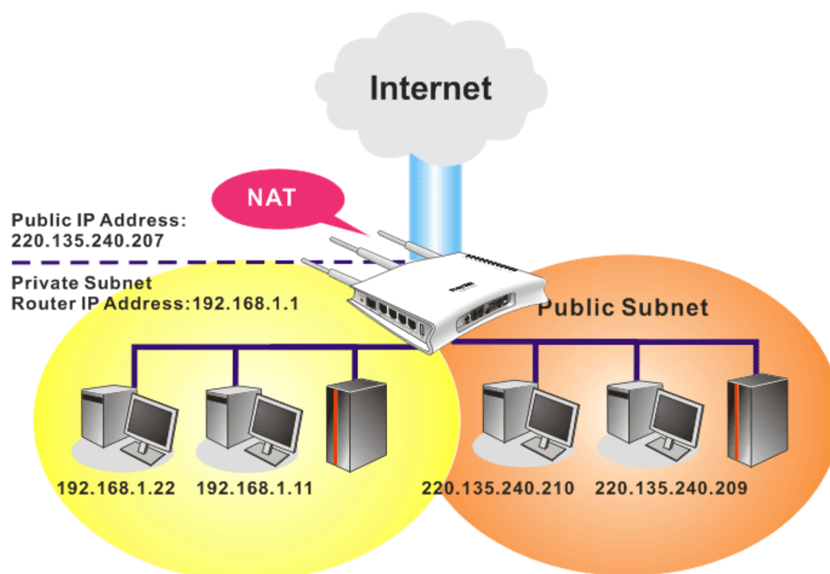



### 4.2.1 區域網路基本概念

Vigor 路由器最基本的功能爲 NAT，可用來建立虛擬的子網路，如前所述，路由器利用真實 IP 位址與網際網路上其他的真實主機互相通訊，或是使用虛擬 IP 地址與區域網路上的主機連繫。NAT 要完成的事情就是轉換來自真實 IP 位址的封包到私有 IP 地址，以便將正確的封包傳送至正確的主機上，反之亦然。此外 Vigor 路由器還有內建的 DHCP 伺服器，可指定虛擬 IP 地址至每個區域主機上，請參考下面的範例圖，即可獲得大略的了解。




在某些特殊的情形當中，您可能會有 ISP 提供給您的真實 IP 子網路像是 220.135.240.0/24，這表示您可以設定一個真實子網路，或是使用配備有真實 IP地址之主機的第二組子網路，作爲真實子網路的一部份，Vigor 路由器將會提供 IP 路由服務，幫助真實地區子網路上的主機能與其他真實主機/外部伺服器溝通連繫，因此路由器必須設定爲真實主機的通訊閘道才行。




## 什麼是 RIP(Routing Information Protocol)

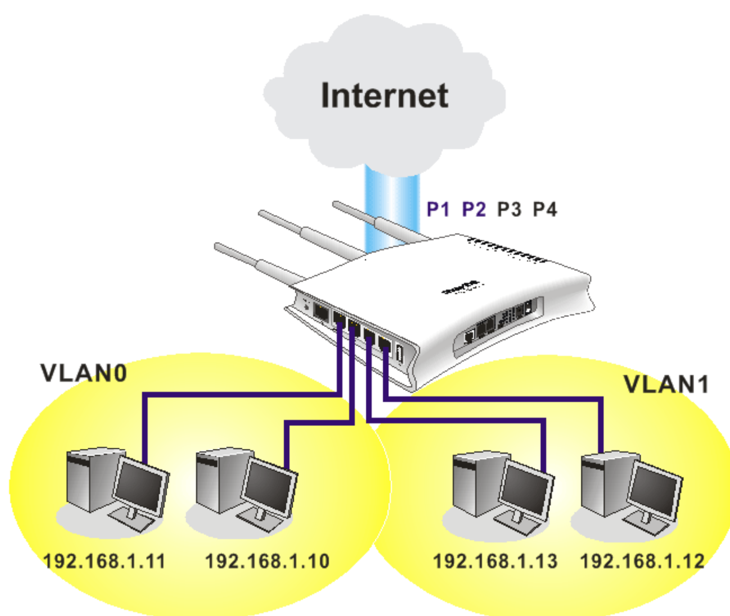
Vigor 路由器可利用 RIP 與鄰近路由器交換路由資訊，達到 IP 路由的目的。這樣可讓使用者變更路由器的資訊，例如 IP 地址，且路由器還會自動通知雙方此類訊息。

## 什麼是固定路由

當您的區域網路上有數個子網路時，比起其他的方法有時候對連線來說最有效也是最快速的方式就是固定路由功能，您可設定一些規則來傳送指定子網路上的資料到另一個指定的子網路上而不需要透過 RIP。

## 什麼是虛擬區域網路(VLAN)

您可以利用實體的連接埠將群組區域網路上的主機，然後建立虛擬區域網路，最多可達 4 個。為了要管理不同群組間的通訊狀況，請再虛擬區域網路功能上設定一些規則，以及每個網路的傳送速率。



### 4.2.2 基本設定

本頁提供您區域網路的基本設定。

按**區域網路**開啓區域網路設定並選擇**基本設定**。

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration
For NAT Usage
1st IP Address 192.168.1.5
1st Subnet Mask 255.255.255.0
For IP Routing Usage ○ Enable ⦿ Disable
2nd IP Address 192.168.2.1
2nd Subnet Mask 255.255.255.0
2nd Subnet DHCP Server
RIP Protocol Control Disable

DHCP Server Configuration
⦿ Enable Server ○ Disable Server
Relay Agent: ○ 1st Subnet ○ 2nd Subnet
Start IP Address 192.168.1.10
IP Pool Counts 50
Gateway IP Address 192.168.1.5
DHCP Server IP Address for Relay Agent

DNS Server IP Address
☐ Force DNS manual setting
Primary IP Address
Secondary IP Address

OK

| | |
|---|---|
| **第一 IP 位址** | 請輸入虛擬 IP 地址以便連接區域虛擬網路(預設値為 192.168.1.1)。 |
| **第一子網路遮罩** | 請輸入決定網路大小的位址碼(預設値為 255.255.255.0/ 24)。 |
| **供 IP 路由使用** | 按下**啓用**以啓動此功能，此功能預設值是**停用**。此應用視情況需要而設定。 |
| **第二 IP 位址** | 請輸入第二組 IP 地址以便連接至子網路(預設値為 192.168.2.1)。 |
| **第二子網路遮罩** | 請輸入第二組決定網路大小的位址碼(預設値為 255.255.255.0/ 24)。 |
| **第二子網路遮罩 DHCP 伺服器** | 您可以將路由器設定為 DHCP 伺服器，提供服務予第二組子網路。 |

http://192.168.1.5 - Router Web Configurator - Microsoft Internet Explorer

2nd DHCP Server

Start IP Address

IP Pool Counts 0 (max. 10)

Index Matched MAC Address given IP Address

MAC Address :

Add Delete Edit Cancel

OK Clear All Close

**起始 IP 位址：**輸入 IP 地址 pool 數值做為 DHCP 伺服器指定 IP 地址時的起始點，如果路由器的第二組 IP 地址為 220.135.240.1,，起始 IP 地址可以是 220.135.240.2 或是更高一些，但比 220.135.240.254 小。

**IP 配置數量：**輸入 IP 地址的數量，最大值為 10，例如您若輸入 3 而第二組 IP 地址為 220.135.240.1，DHCP 伺服器的 IP 地址範圍即為 220.135.240.2 到 220.135.240.4。

**MAC 位址：**請一個個輸入主機的 MAC 地址，按**新增**來建立主機清單以便指定、刪除或是編輯上述範圍中的 IP 地址。設定第二組 DHCP 伺服器所需的 MAC 位址清單，可幫助路由器指定正確的 IP 地址及子網路至正確的主機上。這樣在第二子網路上的主機便不會得到屬於第一組子網路的 IP 地址。

**RIP 協定控制**

**停用 –** 關閉 RIP 協定，可讓不同路由器之間資訊交換暫停（此為預設值)。

RIP Protocol Control Disable

Disable
1st Subnet
2nd Subnet

**第一子網路-**選擇路由器以交換第一子網路和鄰近路由器間的 RIP 資訊。

**第二子網路-**選擇路由器以交換第二子網路和鄰近路由器間的 RIP 資訊。

**DHCP 伺服器組態**

DHCP 是 Dynamic Host Configuration Protocol 的縮寫，路由器的出廠預設值可以作為您的網路的 DHCP 伺服器，所以它可自動分派相關的 IP 設定給區域的使用者，將該使用者設定成為 DHCP 的用戶端。如果您的網路上並沒有任何的 DHCP 伺服器存在，建議您讓路由器以 DHCP 伺服器的型態來運作。

如果您想要使用網路上另外的 DHCP 伺服器，而非路由器的伺服器，您可以利用中繼代理來幫您重新引導 DHCP 需求到指定的位置上。

**啓用 -** 讓路由器指定 IP 地址到區域網路上的每個主機上。

**停用 -** 讓您手動指定 IP 地址到區域網路上的每個主機上。

**DHCP 中繼代理位址 - (1st subnet/2nd subnet)**指定某個 DHCP 伺服器所在的子網路讓中繼代理重新引導 DHCP 需求至該處。

**起始 IP 位址 -** 輸入 DHCP 伺服器的 IP 地址配置的數值作爲指定 IP 地址的起始點，如果第路由器的第一個 IP 地址爲 192.168.1.1，起始 IP 地址可以是 192.168.1.2 或是更高一些，但比 192.168.1.254 小。

**IP 配置數量 -** 輸入您想要 DHCP 伺服器指定 IP 地址的最大數量，預設值爲 50，最大值爲 253。

**閘道 IP 位址 -** 輸入 DHCP 伺服器所需的閘道 IP 地址，這項數值通常與路由器的第一組 IP 地址相同，表示路由器爲預設的閘道。

**DHCP 伺服器 IP 位址關於中繼代理程式 -**設定您預備使用的 DHCP 伺服器 IP 位址，讓中繼代理可以協助傳送 DHCP 需求至伺服器上。

**DNS 伺服器組態**

DNS 是 Domain Name System 的縮寫，每個網際網路的主機都必須擁有獨特的 IP 地址，也必須有人性化且容易記住的名稱諸如 www.yahoo.com 一般，DNS 伺服器可轉換此名稱至相對應的 IP 地址上。

**使用 DNS 手動設定 –** 強迫路由器使用本頁所指定的 DNS 伺服器而非使用網際網路存取伺服器所提供的 DNS 伺服器 (PPPoE, PPTP, L2TP 或 DHCP 伺服器).

**主要 IP 位址 -**您必須在此指定 DNS 伺服器的 IP 地址，因爲通常您的 ISP 應該會提供一個以上的 DNS 伺服器，如果您的 ISP 並未提供，路由器會自動採用預設的 DNS 伺服器 IP 地址 194.109.6.66，放在此區域。

**次要 IP 位址 -** 您可以在此指定第二組 DNS 伺服器 IP 位址，因爲 ISP 業者會提供一個以上的 DNS 伺服器。如果您的 ISP 並未提供，路由器會自動採用預設的第二組 DNS 伺服器，其 IP 位址爲 194.98.0.1，放在此區域。

預設 DNS 伺服器 IP 位址可在線上狀態上查看：

System Status　　System Uptime: 5:11:9

LAN Status　　Primary DNS: 194.109.6.66　　Secondary DNS: 168.95.1.1

| IP Address | TX Packets | RX Packets |
|---|---|---|
| 192.168.1.5 | 9326 | 9487 |

如果主要和次要 IP 地址區都是空白的，路由器將會指定其本身的 IP 地址給予本地使用者作爲 DNS 代理伺服器並且仍保有 DNS 快速緩衝貯存區。

如果網域名稱的 IP 地址已經在 DNS 快速緩衝貯存區內，路由器將立即 resolve 網域名稱。否則路由器會藉著建立 WAN (例如 DSL/Cable)連線時，傳送 DNS 疑問封包至外部 DNS 伺服器。

第五章中舉出二種常見的區域網路設定腳本供您參考，有關設定範例部份，如有需求請參考該章以取得更多的訊息。

### 4.2.3 固定路由

進入**區域網路**群組並選擇**固定路由**，開啓如下的畫面。

LAN >> Static Route Setup

Static Route Configuration | Set to Factory Default | View Routing Table |

| Index | Destination Address | Status | Index | Destination Address | Status |
|---|---|---|---|---|---|
| 1. | ??? | ? | 6. | ??? | ? |
| 2. | ??? | ? | 7. | ??? | ? |
| 3. | ??? | ? | 8. | ??? | ? |
| 4. | ??? | ? | 9. | ??? | ? |
| 5. | ??? | ? | 10. | ??? | ? |

Status: v --- Active, x --- Inactive, ? --- Empty

**索引** 索引下方的號碼(1 到 10)允許您開啓下一層頁面以設定固定路由。

**目標位址** 顯示固定路由的目標位址。

**狀態** 顯示固定路由的狀態。

**檢視路由表** 開啓如下畫面檢視目前的路由狀況。

Diagnostics >> View Routing Table

Current Running Routing Table | Refresh |

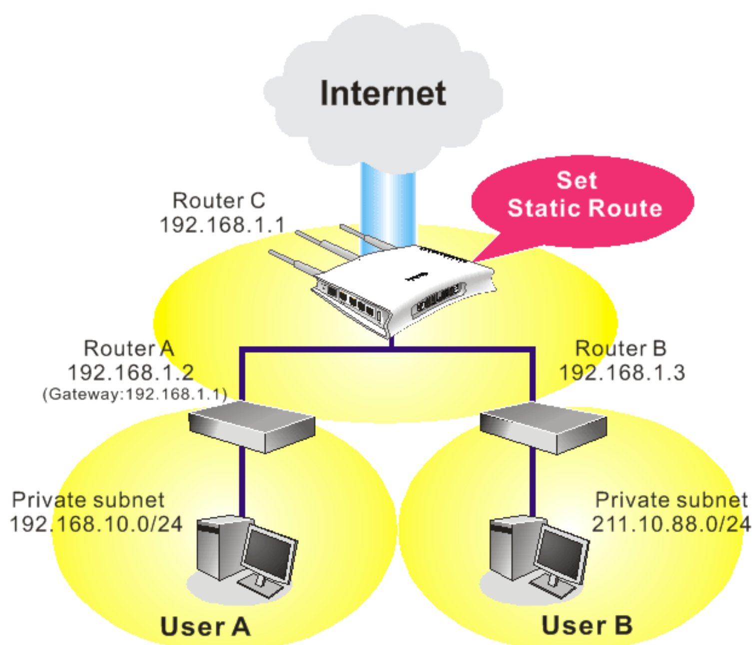
```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
C~        192.168.1.0/    255.255.255.0 is directly connected,     LAN
```

**增加固定路由至虛擬或真實網路上**

此處爲固定路由的範例，不同子網路上的使用者 A 與 B 可以透過路由器彼此溝通。假定網際網路的存取已設定完畢，路由器可以適當的運作。

- 使用主要路由器進入網際網路
- 利用內部的路由器 A(192.168.1.2)，建立虛擬子網路 192.168.10.0
- 透過內部的路由器 B(192.168.1.3)，建立真實子網路 211.100.88.0
- 已設定主要路由器 192.168.1.1 爲路由器 A (192.168.1.2) 的預設閘道

在設定固定路由之前，使用者 A 無法與使用者 B 溝通，因爲路由器 A 只會傳送辨認出的封包至主要路由器的預設閘道。




1. 在**區域網路**群組中，選擇**一般設定**。再選擇第一子網路作爲 **RIP 協定控制**，然後點選**確定**按鈕。

   > **注意**：有二個理由讓我們一定要在第一子網路上應用 RIP 通訊協定。第一個理由是區域網路介面可以透過第一子網路(192.168.1.0/24)與鄰近路由器作 RIP 封包交換，第二個，理由是網際網路虛擬子網路上(例如 192.168.10.0/24)的主機群可以藉此路由器存取網際網路資訊，並和不同子網路持續進行 IP 路由資訊交換。

2. 在**區域網路**群組中，選擇固定路由，按索引編號 1 勾選**啓用**方塊， 請以下列數字新增一個固定路由，讓所有應前往 192.168.10.0 的封包都能透過 192.168.1.2 來轉送，接著按**確定**。

   LAN >> Static Route Setup

   Index No. 1

   ☑ Enable

   | | |
   |---|---|
   | Destination IP Address | 192.168.10.0 |
   | Subnet Mask | 255.255.255.0 |
   | Gateway IP Address | 192.168.1.2 |
   | Network Interface | LAN |

   OK　Cancel

3. 回到**固定路由**頁面，按另一個索引編號增加另一個固定路由，設定如下圖。它可將所有指定前往 211.100.88.0 的封包轉送至 192.168.1.3，然後按**確定**。

LAN >> Static Route Setup

Index No. 1

☑ Enable

| | |
|---|---|
| Destination IP Address | 211.100.88.0 |
| Subnet Mask | 255.255.255.0 |
| Gateway IP Address | 192.168.1.3 |
| Network Interface | LAN |

OK　Cancel

4. 按**診斷工具**中的**路由表**檢查目前的路由表格。

Diagnostics >> View Routing Table

Current Running Routing Table　| Refresh |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
S~       192.168.10.0/   255.255.255.0 via 192.168.1.2,     LAN
C~        192.168.1.0/   255.255.255.0 is directly connected,    LAN
S~       211.100.88.0/   255.255.255.0 via 192.168.1.3,     LAN
```

## 4.2.5 綁定 IP 與 MAC 位址

此功能用來綁定區域網路中的電腦之 IP 與 MAC 位址，如此一來可在網路上達到更有效的控制。當此一功能啓用時，所有被綁定的 IP 與 MAC 位址的電腦都不能在變更，如果您修改了綁定 IP 或 MAC 位址，可能會造成無法存取網際網路的窘態。

按 **LAN** 並選擇**綁定 IP 至 MAC** 開啓設定網頁。

LAN >> Bind IP to MAC

**Bind IP to MAC**

Note: IP-MAC binding presets DHCP Allocations.
If you select Strict Bind, unspecified LAN clients cannot access the Internet.

◉ Enable ○ Disable ○ Strict Bind

ARP Table | Select All | Sort | Refresh |

| IP Address | Mac Address |
|---|---|
| 192.168.1.1 | 00-50-7F-DD-15-18 |
| 192.168.1.10 | 00-0E-A6-2A-D5-A1 |

IP Bind List | Select All | Sort |

| Index | IP Address | Mac Address |
|---|---|---|

Add and Edit

IP Address

Mac Address : : : : :

Add Edit Delete

OK

| | |
|---|---|
| **啓用** | 按此鈕啓用此功能，不過未列在 IP 綁定清單中的 IP/MAC 位址以可以連上網際網路。 |
| **停用** | 按此鈕關閉此功能，頁面上全部的設定都將會失效。 |
| **限制綁定** | 按此鈕封鎖未列在 IP 綁定清單中的 IP/MAC 位址連線。 |
| **ARP 表** | 此表格爲路由器的區域網路 ARP 表，IP 和 MAC 資訊將顯示於本區。列於 ARP 表中的每組 IP 和 MAC 位址都可以爲使用者挑選並透過新增按鈕加到 IP 綁定清單上。 |
| **全選** | 按此連結選擇表格內全部內容。 |
| **排序** | 按此連結將表格內容按照 IP 位址重新排序。 |
| **更新頁面** | 用來更新 ARP 表格，當新的電腦增加到區域網路上時，您可以按此連結取得最新的 ARP 表格資訊。 |
| **新增與編輯** | **IP 位址** – 輸入 IP 位址以作爲指定 MAC 位址之用。<br>**MAC 位址** – 輸入 MAC 位址以便與指定的 IP 位址綁在一起。 |
| **IP 綁定清單** | 顯示綁定 IP 至 MAC 資訊清單。 |
| **新增** | 允許您將 ARP 表格中所挑選的或是在新增和編輯上所輸入的 IP/MAC 位址新增至 **IP 綁定清單**上。 |
| **編輯** | 允許您編輯或修正先前所建立的 IP 位址和 MAC 位址。 |
| **刪除** | 您可以刪除 **IP 綁定清單**上任何一個項目，選擇您想刪除的項目然後按**刪除**按鈕，選定的項目將自 **IP 綁定清單**上刪除。 |

**附註:** 在您選擇**限制綁定**前，您必須爲一台電腦設定一組 IP/MAC 位址，若無設定的話，沒有一台電腦可以連上網際網路，路由器的網頁組態設定也無法進入了。

# 4.3 NAT

通常，路由器可以 NAT 路由器提供其相關服務，NAT 是一種機制，一個或多個虛擬 IP 位址可以對應到某個單一的真實 IP 位址。真實 IP 位址習慣上是由您的 ISP 所指定的，因此您必須爲此負擔費用，虛擬 IP 位址則只能在內部主機內辨識出來。

當封包之目的地位址爲網路上某個伺服器時，會先送到路由器，路由器即改變其來源位址，成爲真實 IP 位址，並透過真實通訊埠傳送出去。同時，路由器在連線數表格中列出清單，以記錄位址與通訊埠對應的相關資訊，當伺服器回應時，資料將直接傳回路由器的真實 IP 位址。

NAT 的好處如下：

- **於應用真實 IP 位址上節省花費以及有效利用 IP 位址** NAT 允許本機中的 IP 位址轉成真實 IP 位址，如此一來您可以一個 IP 位址來代表本機。
- **利用隱匿的 IP 位址強化內部網路的安全性** 有很多種攻擊行動都是基於 IP 位址而對受害者發動的，既然駭客並不知曉任何虛擬 IP 位址，那麼 NAT 功能就可以保護內部網路不受此類攻擊。

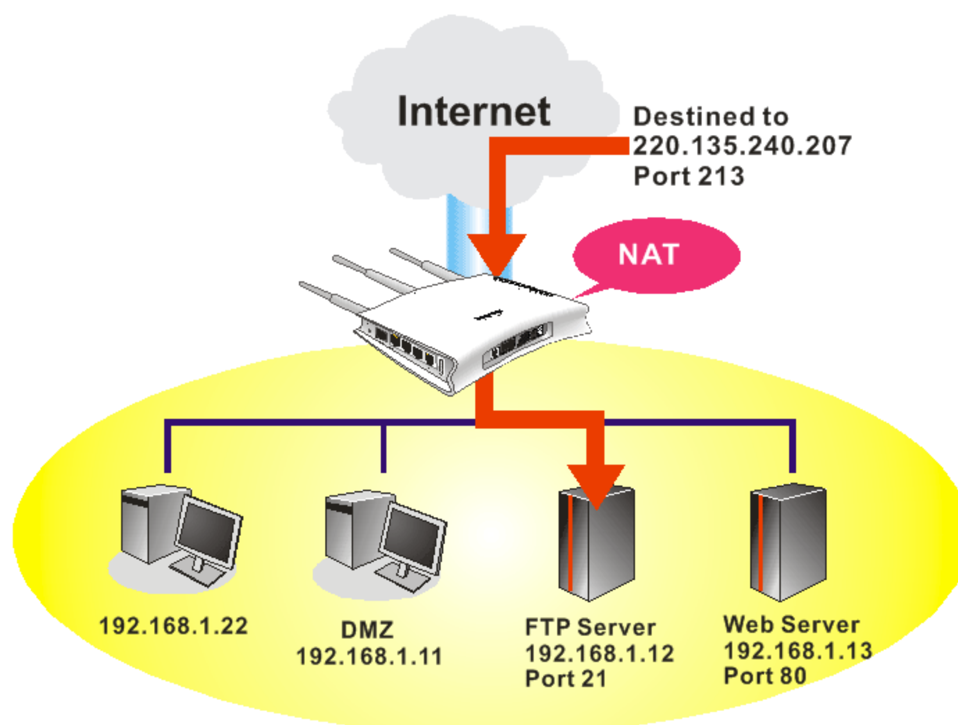
在 NAT 頁面中，您將可看見以 RFC-1918 定義的虛擬 IP 位址，通常我們會使用 192.168.1.0/24 子網路給予路由器使用。就如前所提及的一般，NAT 功能可以對應一或多個 IP 位址和/或服務通訊埠到不同的服務上，換句話說，NAT 功能可以利用通訊埠對應方式來達成。

下圖爲 NAT 功能項目：




## 4.3.1 通訊埠重導向

**通訊埠重導向**通常是爲了本地區域網路中的網頁伺服器、FTP 伺服器、E-mail 伺服器等相關服務而設定，大部分的情形是您需要給每個伺服器一個真實 IP 位址，此一真實 IP 位址/網域名稱可以爲所有使用者所辨識。既然此伺服器實際坐落於區域網路內，因此網路可以受到路由器之 NAT 的詳密保護，且可由虛擬 IP 位址/通訊埠來辨認。通訊埠重導向表的功能是傳送所有來自外部使用者對真實 IP 位址之存取需求，以對應至伺服器的虛擬 IP 位址/通訊埠。




**通訊埠重導向**只能應用在流入的資料量上。

欲使用此項功能，請開啓 **NAT** 頁面然後選擇**通訊埠重導向。通訊埠重導向**提供 10 組通訊埠對應入口給予內部主機對應使用。

NAT >> Port Redirection

Port Redirection | Set to Factory Default |

| Index | Service Name | Public Port | Private IP | Status |
|---|---|---|---|---|
| 1. | | | | x |
| 2. | | | | x |
| 3. | | | | x |
| 4. | | | | x |
| 5. | | | | x |
| 6. | | | | x |
| 7. | | | | x |
| 8. | | | | x |
| 9. | | | | x |
| 10. | | | | x |

<< 1-10 | 11-20 >> Next >>

按下索引編號下的號碼連結，進入次層之設定頁面:

NAT >> Port Redirection

Index No. 1

☐ Enable

| | |
|---|---|
| Mode | Single / Single, Range |
| Service Name | |
| Protocol | --- |
| WAN IP | 1.All |
| Public Port | 0 |
| Private IP | |
| Private Port | 0 |

Note: In "Range" Mode the End IP will be calculated automatically once the Public Port and Start IP have been entered.

OK Clear Cancel

| | |
|---|---|
| **啓用** | 勾選此方塊啓用此通訊埠重導向設定。 |
| **模式** | 有二種模式可以供使用者選擇，如欲設定範圍給予指定服務，請選擇**範圍**。在"範圍" 模式下，若 IP 位址與第一個對外通訊埠號皆填入之後，系統將自動計算並顯示第二個對外通訊埠值。 |
| **服務名稱** | 輸入特定網路服務的名稱。 |
| **通訊協定** | 選擇傳送層級的通訊協定(TCP 或 UDP)。 |
| **對外通訊埠** | 指定哪一個通訊埠可以重新導向至內部主機特定的虛擬 IP 通訊埠上。如果您選擇**範圍**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入需要的數值，系統將會自動指定數值予第二個方塊。 |
| **虛擬 IP** | 指定提供服務的主機之 IP 位址，如果您選擇**範圍**作爲重導向模式，您將會在此看見二個方塊，請在第一個方塊輸入完整的 IP 位址 (作爲起點)，在第二個方塊輸入四位數字(作爲終點)。 |
| **虛擬通訊埠** | 指定內部主機提供服務之虛擬通訊埠號。 |

注意路由器有其內建服務(伺服器)諸如 Telnet、HTTP 和 FTP，因爲這些服務(伺服器)的通訊埠號幾乎都相同，因此您可能需要重新啓動路由器以避免衝突發生。

例如，路由器的內建網頁設定給予的設定值是埠號 80，它可能造成與本地網路中網頁伺服器 http://192.168.1.13:80 產生衝突，因此您需要改變路由器的 **http** 通訊埠號，除了 80 以外任何一種都可以（例如 8080），來防止衝突發生。在系統管理群中的管理設定可以做此調整，接著您可在 IP 位址尾端加入 8080 (如 http://192.168.1.1:8080 而非僅只通訊埠號 80)來進入管理畫面。

System Maintenance >> Management

Management Setup

| Management Access Control | Management Port Setup | | |
|---|---|---|---|
| ☑ Allow management from the Internet | ◉ User Define Ports ○ Default Ports | | |
| ☐ FTP Server | Telnet Port | 23 | (Default: 23) |
| ☑ HTTP Server | HTTP Port | 80 | (Default: 80) |
| ☑ HTTPS Server | HTTPS Port | 443 | (Default: 443) |
| ☑ Telnet Server | FTP Port | 21 | (Default: 21) |
| ☐ SSH Server | SSH Port | 22 | (Default: 22) |
| ☑ Disable PING from the Internet | | | |

Access List

| List | IP | Subnet Mask |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |

SNMP Setup

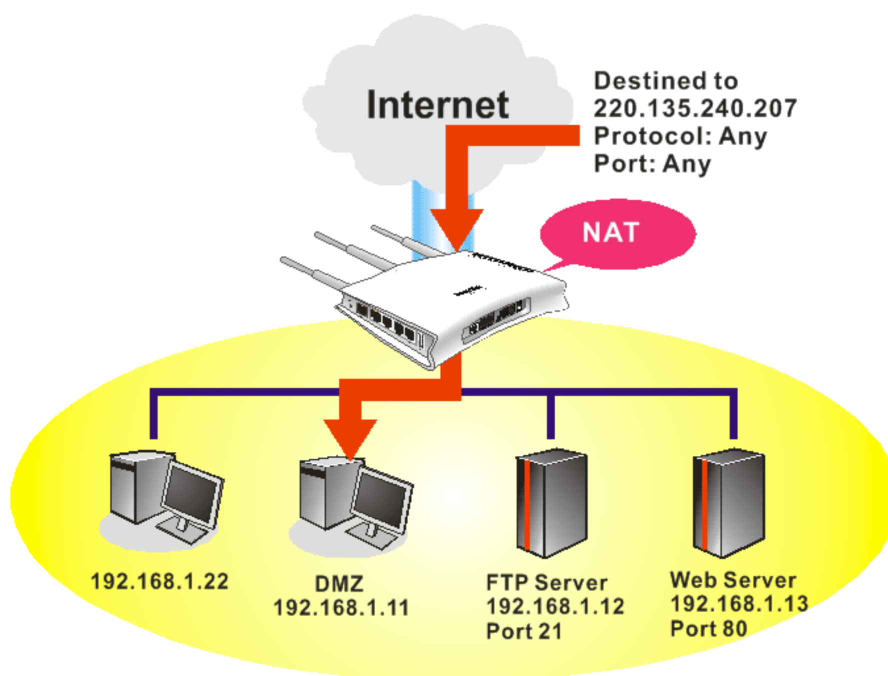
☐ Enable SNMP Agent

| | | |
|---|---|---|
| Get Community | public | |
| Set Community | private | |
| Manager Host IP | | |
| Trap Community | public | |
| Notification Host IP | | |
| Trap Timeout | 10 | seconds |

OK

## 4.3.2 DMZ 主機設定

如同上面所提及的內容，通訊埠重導向可以將流入的 TCP/UDP 或是特定通訊埠中其他的流量，重新導向區域網路中特定主機之 IP 位址/通訊埠。不過其他的 IP 協定例如協定 50 (ESP)和 51(AH)是不會在固定通訊埠上行動的，Vigor 路由器提供一個很有效的工具 DMZ 主機，可以將任何協定上的需求資料對應到區域網路的單一主機上。來自用戶端的正常網頁搜尋和其他網際網路上的活動將可繼續進行，而不受到任何打擾。DMZ 主機允許內部被定義規範的使用者完全暴露在網際網路上，通常可促進某些特定應用程式如 Netmeeting 或是網路遊戲等等的進行。




> **注意**：NAT 固有的安全性屬性在您設定 DMZ 主機時稍微被忽略了，建議您另外新增額外的過濾器規則或是第二組防火牆。

請按 **DMZ 主機設定**開啓下述頁面：

NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

None

Private IP　　Choose PC

MAC Address of the True IP DMZ Host　00 . 00 . 00 : 00 . 00 . 00

Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on.

OK

如果您在**網際網路連線設定**選擇 **PPPoE/固定 IP/PPTP**，並且設定 **WAN 別名**，您將可在此頁面發現**輔助 WAN IP** 項目。

NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

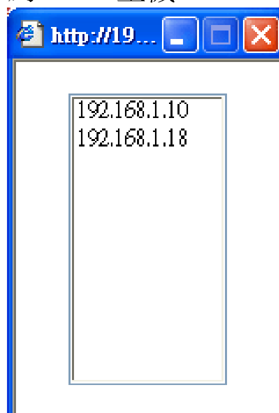
| Index | Enable | Aux. WAN IP | Private IP | |
|---|---|---|---|---|
| 1. | ☐ | 172.16.3.229 | | Choose PC |
| 2. | ☐ | 162.168.1.55 | | Choose PC |

OK　Clear

**開啓**　　勾選此項以啓動 DMZ 主機功能。

**虛擬 IP** 輸入 DMZ 主機的虛擬 IP 位址，或是按**選擇 PC** 開啓另一頁面來選擇。

**選擇電腦** 按下此鈕後，如下視窗立即跳出。此視窗包含您的區域網路中全部主機的虛擬 IP 位址清單，請自清單中選擇一個虛擬 IP 位址作爲 DMZ 主機。




當您已經從上面的視窗選好了虛擬 IP 位址時，該 IP 位址將會顯示在下面的螢幕上，請按**確定**儲存這些設定。

NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

| Index | Enable | Aux. WAN IP | Private IP | |
|---|---|---|---|---|
| 1. | ☑ | 172.16.3.229 | 192.168.1.10 | Choose PC |
| 2. | ☐ | 162.168.1.55 | | Choose PC |

OK Clear

## 4.3.3 開放通訊埠

**開放通訊埠**允許您開啓一段範圍內的通訊埠，供特定應用程式使用。常見的應用程式包含有 P2P 應用程式(如 BT、KaZaA、Gnutella、WinMX、eMule 和其他)、Internet Camera 等等，您需要先確定應用程式包含最新的資料，以免成爲安全事件的受害者。

按**開放通訊埠**連結開啓下面的網頁。

NAT >> Open Ports

Open Ports Setup | Set to Factory Default |

| Index | Comment | Aux. WAN IP | Local IP Address | Status |
|---|---|---|---|---|
| 1. | | | | x |
| 2. | | | | x |
| 3. | | | | x |
| 4. | | | | x |
| 5. | | | | x |
| 6. | | | | x |
| 7. | | | | x |
| 8. | | | | x |
| 9. | | | | x |
| 10. | | | | x |

<< 1-10 | 11-20 >> Next >>

**索引** 表示本地主機中您想要提供之服務，其特定內容網頁之相關號碼，您應該選擇適當的索引號碼以編輯或是清除相關的內容。

**註解** 指定特定網路服務的名稱。

**WAN 介面** 顯示該項設定之 WAN 介面。

**內部 IP 位址** 顯示提供此項服務之本地主機的 IP 位址。

**狀態** 顯示每項設定的狀態，X 或 V 表示關閉或是啓用狀態。

如果要新增或是編輯通訊埠設定，請按索引下方的號碼按鈕。該索引號碼入口設定頁面隨即出現，在每個輸入頁面中，您可以指定 **10** 組通訊埠範圍給予不同的服務。

NAT >> Open Ports >> Edit Open Ports

Index No. 1

☑ Enable Open Ports

Comment: P2P

WAN IP: 172.16.3.229

Local Computer: 192.168.1.10 [Choose PC]

| | Protocol | Start Port | End Port | | Protocol | Start Port | End Port |
|---|---|---|---|---|---|---|---|
| 1. | TCP | 4500 | 4700 | 6. | ----- | 0 | 0 |
| 2. | UDP | 4500 | 4700 | 7. | ----- | 0 | 0 |
| 3. | ----- | 0 | 0 | 8. | ----- | 0 | 0 |
| 4. | ----- | 0 | 0 | 9. | ----- | 0 | 0 |
| 5. | ----- | 0 | 0 | 10. | ----- | 0 | 0 |

[OK] [Clear] [Cancel]

**啓用開放通訊埠** 勾選此項以啓動此功能。

**說明** 請爲所定義的網路應用/服務命名。

**本機電腦** 輸入本機的虛擬 IP 位址或是按**選擇電腦**挑選另外一個。

**選擇電腦** 按此鈕後另一個視窗即自動跳出並提供本機的虛擬 IP 位址之清單資料，請自清單中選取最適宜的 IP 位址。

**通訊協定** 指定傳送層級的通訊協定，有 **TCP**、**UDP** 和 **----- (none)**等幾種選擇。

**起始通訊埠** 指定本機所提供之服務的開始通訊埠號。

**結束通訊埠** 指定本機所提供之服務的結束通訊埠號。

## 4.4 硬體加速

## 4.5 防火牆

### 4.5.1 防火牆基本常識

當寬頻使用者需要更多的頻寬以便用於多媒體、應用程式或是遠程學習時，安全性總是最受到重視的一環。Vigor 路由器的防火牆可以協助保護您本地網路免受外在人物的攻擊，同時它可限制本地網路的使用者存取網際網路。此外它還可以過濾一些由觸發路由器所建立的連線特定封包。

最基本的安全觀念就是在您安裝路由器時，設定使用者名稱和密碼。管理者登入可以防止未授權用戶從您的路由器登入並更改存取路由器設定。

## 防火牆工具

區域網路上的使用者可以下述的防火牆工具，接受良好的安全防護：

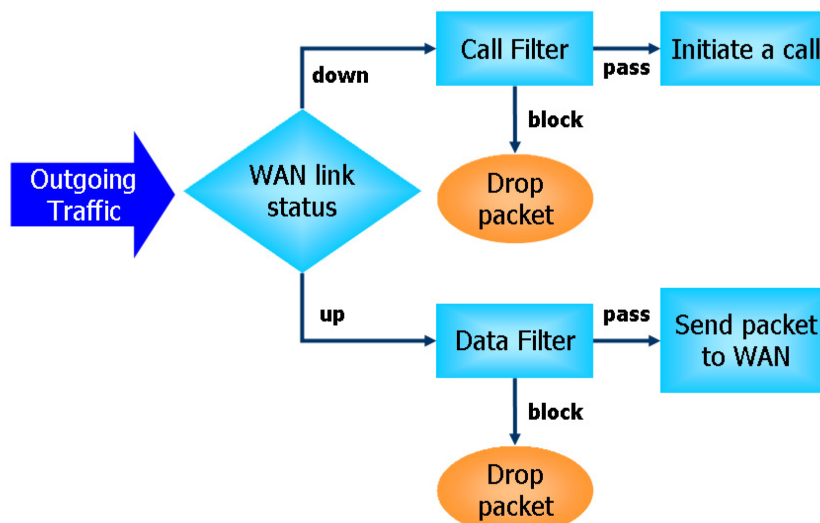
- 用戶設定 IP 過濾器(呼叫過濾器/資料過濾器)
- Stateful Packet Inspection (SPI): 追蹤封包並阻擋未經要求而流入的資料
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS)攻擊防禦
- URL 內容過濾器

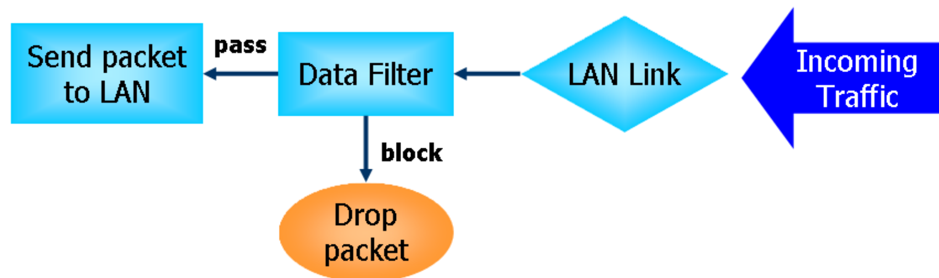
## IP 過濾器

依照現有網際網路連線的需求、廣域網路連接狀態(開啓或關閉)的情形，IP 過濾器結構可將資料流量分成二大類：呼叫過濾器和資料過濾器。

- **呼叫過濾器** -當目前前沒有任何網際網路連線時，呼叫過濾器可應用在所有的資料運輸流量上，所有的運輸應該是往外送出。系統會按照過濾器規則檢查封包，如果是合法的，該封包即可通過，然後路由器將啓動一次呼叫來建立網際網路連線，再將該封包傳送往網際網路。
- **資料過濾器** - 網際網路正處於連線狀態時，資料過濾器可應用在流入與流出的資料傳輸上，系統會按照過濾器規則檢查封包，如果是合法的，該封包即可通過。

以下圖表解釋流入與流出之資料傳輸程序。






### 封包狀態檢測(SPI)

在網路層級上，封包狀態檢測是一種防火牆結構，它會建立一個封包狀態機器來追蹤防火牆於所有介面的連線狀況，並確保這些連線都是有效的。此類型防火牆並不只是檢查封包標頭資訊，它同時也監視著連線的狀態。

### 數位內容安全管理(Content Security Management, CSM)

因爲立即通訊應用程式蓬勃的發展，人與人間的通訊變得越來越容易。然而一些企業利用此種程式作爲與客戶通訊的有力工具時，部分公司對此可能還是抱持保留態度，這是因爲他們想要減少員工在上班時間誤用此程式或是防止未知的安全漏洞發生。對於準備應用點對點程式的公司來說，情況也是相同的，因爲檔案分享可以很方便但是同時也很危險。爲了應付這些需求，我們提供了 CSM 阻擋功能。

### DoS 攻擊防禦

DoS 攻擊防禦功能協助用戶檢測並減輕 DoS 攻擊，這類攻擊通常可分成二大類 – flood 類型攻擊和弱點攻擊。flood 類型攻擊嘗試耗盡您的系統資源，而弱點攻擊則是利用通訊協定或是操作系統的弱點嘗試癱瘓系統。

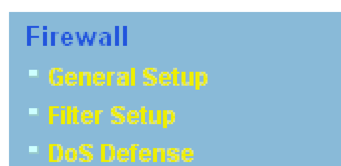
DoS 攻擊防禦功能的引發是以 Vigor 路由器的攻擊特徵值資料庫爲基礎，執行每一個封包的檢查，任何可能重複產生以癱瘓主機之惡意封包，在安全的區域網路中都將嚴格阻擋，如果您有設定系統紀錄伺服器，那麼系統紀錄訊息也會傳送警告資訊給您。

Vigor 路由器也可以監視資料流量，任何違反事先定義的參數的不正常資料流(例如臨界值的數字)，都會被視爲是一種攻擊行爲，Vigor 路由器將啓動防衛機制，及時阻擋減輕災害。

下列表格顯示出 DoS 攻擊防禦功能所能檢測出的攻擊類型。

1. SYN flood 攻擊
2. UDP flood 攻擊
3. ICMP flood 攻擊
4. Port Scan 攻擊
5. IP options
6. Land 攻擊
7. Smurf 攻擊
8. 路由追蹤
9. SYN 封包片段攻
10. Fraggle 攻擊
11. TCP flag scan
12. Tear drop 攻擊
13. Ping of Death 攻擊
14. ICMP 封包片段攻
15. 未知通訊協定

下圖爲防火牆的功能項目：




## 4.5.2 基本設定

**基本設定**允許您調整 IP 過濾器和一般選項的設定內容，在此頁面您可以啓動或是關閉**呼叫過濾器**或**資料過濾器**。在某些情況下，您的過濾器可利用連結的方式執行一系列過濾工作，因此在這裡，您只要指定**開始過濾器組別**即可。當然，您也可以調整紀錄模式設定以及勾選**接受流入的 UDP Fragment 封包**。

自**防火牆**群中選擇**基本設定**連結。

Firewall >> General Setup

General Setup

| | | | |
|---|---|---|---|
| Call Filter | ⦿ Enable | Start Filter Set | Set#1 |
| | ○ Disable | | |
| Data Filter | ⦿ Enable | Start Filter Set | Set#2 |
| | ○ Disable | | |

Actions for default rule:

| Application | Action/Profile | Syslog |
|---|---|---|
| Filter | Pass | ☐ |
| IM/P2P Filter | None | ☐ |
| URL Content Filter | None | ☐ |
| Web Content Filter | None | ☐ |

Advance Setting　Edit

☑ Accept large incoming fragmented UDP or ICMP packets ( for some games, ex. CS )

OK　Cancel

**呼叫過濾器**　選擇**啟用**以啟動呼叫過濾器功能，並指定開始過濾器組別。

**資料過濾器**　選擇**啟用**以啟動資料過濾器功能，並指定開始過濾器組別。

**過濾器**　本頁可是定預設規則.
**通過** – 所有的封包都可通過路由器，不需考慮**防火牆>>過濾器**的設定內容。
**封鎖** - 所有的封包都不許通過路由器，且不需考慮**防火牆>>過濾器**的設定內容。

Pass
Pass
Block

一些線上遊戲都會使用很多的片段 UDP 封包來傳送遊戲資料，出於安全防火牆的本能直覺，Vigor 路由器會將這些片段封包給退回，以避免攻擊發生，除非您啟動**接受流入的大量 UDP 或是 ICMP Fragment 封包**，勾選此方塊後，您就可以在這些線上遊戲上優遊。如果安全利害關係具有較高的重要性，您就不要啟動**接受流入的大量 UDP 或是 ICMP Fragment 封包**功能。

## 4.5.3 過濾器設定

按**防火**牆並選擇**過濾器設定**以開啟如下的設定網頁。

Firewall >> Filter Setup

Filter Setup　| Set to Factory Default |

| Set | Comments | Set | Comments |
|---|---|---|---|
| 1. | Default Call Filter | 7. | |
| 2. | Default Data Filter | 8. | |
| 3. | | 9. | |
| 4. | | 10. | |
| 5. | | 11. | |
| 6. | | 12. | |

如果要新增一個過濾器，請按組別下方的數字按鈕以便編輯個別設定。如下的頁面將立即出現，每一個過濾器都含有 7 組規則，請按規則按鈕編輯每個規則，勾選**啓用**則可啓動該項規則。

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments : Default Call Filter

| Filter Rule | Active | Comments | Move Up | Move Down |
|---|---|---|---|---|
| 1 | ☑ | Block NetBios | | Down |
| 2 | ☐ | | UP | Down |
| 3 | ☐ | | UP | Down |
| 4 | ☐ | | UP | Down |
| 5 | ☐ | | UP | Down |
| 6 | ☐ | | UP | Down |
| 7 | ☐ | | UP | |

Next Filter Set None

OK Clear Cancel

**過濾器規則** 請按號碼按鈕(1 ~ 7)編輯過濾器的規則，按下此鈕可以開啓過濾器規則網頁，有關詳細的資訊，請參考稍後的說明。

**啓用** 啓動或是關閉此項過濾規則。

**註解** 輸入過濾規則註解說明，最大長度可以達到 23 個字元。

**上移/下移** 使用上下連結來移動過濾器規則的順序。

**下一個過濾器組別** 設定前往下一個執行的過濾器連結，請勿讓多個過濾器設定形成一個迴路。

欲編輯**過濾器規則**，請按過濾器規則索引按鈕以便進入過濾器規則設定網頁。

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

☑ Check to enable the Filter Rule

| | |
|---|---|
| Comments: | Block NetBios |
| Index(1-15) in Schedule Setup: | , , , |
| Direction: | LAN -> WAN |
| Source IP: | Any (Edit) |
| Destination IP: | Any (Edit) |
| Service Type: | TCP/UDP, Port: from 137~139 to undefined (Edit) |
| Fragments: | Don't Care |

| Application | Action/Profile | Syslog |
|---|---|---|
| Filter: | Block Immediately | ☐ |
| Branch to Other Filter Set: | None | |
| IM/P2P Filter: | None | ☐ |
| URL Content Filter | None | ☐ |
| Web Content Filter | None | ☐ |

Advance Setting Edit

OK Clear Cancel

| | |
|---|---|
| **啓用過濾規則** | 勾選此項目以啓動過濾規則。 |
| **註解** | 輸入過濾器設定註解說明，最大長度爲 14 個字元。 |
| **索引號碼 (1-15)** | 設定區域網路上的電腦工作的時間間隔，您可以輸入四組時間排程，所有的排程都可在**應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。 |
| **方向** | 設定封包流向的方向(LAN->WAN/WAN->LAN)，此項設定僅適用**資料過濾器**，對於呼叫過濾器而言，這項設定是不適用的。 |

**來源/目的 IP** 按下**編輯**進入如下的畫面，選擇來源/目標 IP 或是 IP 範圍。

**服務類型**

按**編輯**進入如下的畫面，以選擇適合之服務類型。

欲手動設定服務類型，請選擇使用者自訂做為服務類型，並輸入相關的設定資料，此外如果您想要使用群組或是物件中所定義的服務類型，請選擇**群組與物件**作為服務類型。

**協定** -指定本過濾器規則套用的協定。

**來源/目標通訊埠** -

**(=)** – 當起始埠號與結束埠號與的數值相同時，此符號表示一個通訊埠。當起始埠號與結束埠號的數值不同時，即表示設定檔所適用的通訊埠範圍。

**(!=)** –當起始埠號與結束的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當起始埠號與結束埠號數值不同時，即除了此處所設定的範圍以外，所有的通訊埠都適用於此設定檔。

**(>)** – 大於此數值的通訊埠號皆可使用。

**(<)** – 小於此數值的通訊埠號皆可使用。

**服務群組/物件** - 使用下拉式選項選擇所需的項目。

**片段**

指定片段封包的執行動作，這個項目也是僅針對**資料過濾器**。

**忽略** - 不論是怎樣的片端封包，系統皆不採取行動。

**無片段** - 應用規則至無片段之封包上。

**片段**- 應用規則至片段之封包上。

**太短了** - 只有過短無法包含完整封包頭之封包，可應用此規則。

**過濾器**

指定系統針對符合規則之封包所採取的行動。

**立刻通過**- 符合規則之封包可立即通過。

**立刻封鎖** - 系統封鎖符合規則之封包。

**若無符合其於規則即通過** - 符合限定規則且並未符合其他規則之封包可立即通過。

**若無符合其於規則即封鎖** - 系統封鎖符合限定規則且並未符合其他規則之封包。

基於疑難排除的需要，您可指定記錄過濾器資訊，只要勾選 **Syslog** 方框即可。

**分至其他過濾器設定** 封包符合過濾器規則，下一個過濾器規則將分至指定之過濾器設定。請自下拉式選項中選擇下一個過濾器規則以便做分支動作，要注意路由器將會採用指定之過濾器規則，且絕對不會回到先前所設定之過濾器規則。

**SysLog** 基於疑難排除的需要，您可指定記錄過濾器資訊

## Example

如上所言，全部的資料傳輸都將以二種 IP 過濾器(呼叫過濾器或是資料過濾器）來分開執行，您可以設定 12 組呼叫過濾器和資料過濾器，每種過濾器設定由 7 種過濾器規則組合而成，這些規則都是事前定義完成。然後在**基本設定**中， 您可以指定一組規則予呼叫過濾器與資料過濾器使用。

Firewall >> General Setup

General Setup

Call Filter ◉ Enable ○ Disable Start Filter Set Set#1

Data Filter ◉ Enable ○ Disable Start Filter Set Set#2

Actions for default rule:

| Application | Action/Profile | Syslog |
|---|---|---|
| Filter | Pass | ☐ |
| IM/P2P Filter | None | ☐ |
| URL Content Filter | None | ☐ |
| Web Content Filter | None | ☐ |

Advance Setting Edit

☑ Accept large incoming fragmented UDP or ICMP packets ( for some games, ex. CS )

OK Cancel

Firewall >> Filter Setup

Filter Setup | Set to Factory Default |

| Set | Comments | Set | Comments |
|---|---|---|---|
| 1. | Default Call Filter | 7. | |
| 2. | Default Data Filter | 8. | |
| 3. | | 9. | |
| 4. | | 10. | |
| 5. | | 11. | |
| 6. | | 12. | |

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments : Default Call Filter

| Filter Rule | Active | Comments | Move Up | Move Down |
|---|---|---|---|---|
| 1 | ☑ | Block NetBios | | |
| 2 | ☐ | | UP | |
| 3 | ☐ | | UP | |
| 4 | ☐ | | UP | |
| 5 | ☐ | | UP | |
| 6 | ☐ | | UP | |
| 7 | ☐ | | UP | |

Next Filter Set

OK Clear Cancel

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

☑ Check to enable the Filter Rule

Comments: Block NetBios

Index(1-15) in Schedule Setup:

Direction: LAN -> WAN

Source IP: Any Edit

Destination IP: Any Edit

Service Type: TCP/UDP, Port: from 137~139 to undefined Edit

Fragments: Don't Care

| Application | Action/Profile | Syslog |
|---|---|---|
| Filter: | Block Immediately | ☐ |
| Branch to Other Filter Set: | None | |
| IM/P2P Filter: | None | ☐ |
| URL Content Filter | None | ☐ |
| Web Content Filter | None | ☐ |

Advance Setting Edit

OK Clear Cancel

## 4.5.4 DoS 攻擊防禦功能設定

這是 **IP 過濾程式/防火牆**的次功能選項，有 15 種檢測/防禦功能類型，DoS 攻擊防禦功能的預設值是關閉的。

按**防火牆**並選擇 **DoS 攻擊防禦功能**開啓設定網頁。

Firewall >> DoS defense Setup

DoS defense Setup

☑ Enable DoS Defense

| | | | |
|---|---|---|---|
| ☐ Enable SYN flood defense | Threshold | 50 | packets / sec |
| | Timeout | 10 | sec |
| ☐ Enable UDP flood defense | Threshold | 150 | packets / sec |
| | Timeout | 10 | sec |
| ☐ Enable ICMP flood defense | Threshold | 50 | packets / sec |
| | Timeout | 10 | sec |
| ☐ Enable Port Scan detection | Threshold | 150 | packets / sec |

| | |
|---|---|
| ☐ Block IP options | ☐ Block TCP flag scan |
| ☐ Block Land | ☐ Block Tear Drop |
| ☐ Block Smurf | ☐ Block Ping of Death |
| ☐ Block trace route | ☐ Block ICMP fragment |
| ☐ Block SYN fragment | ☐ Block UnknownProtocol |
| ☐ Block Fraggle Attack | |

Enable DoS defense function to prevent the attacks from hacker or crackers.

OK　Clear All　Cancel

| | |
|---|---|
| **啓用** | 勾選此項以啓動 DoS 攻擊防禦功能。 |
| **啓用 SYN flood 攻擊防禦功能** | 勾選此項以啓動 SYN 攻擊防禦功能，一旦檢查到 TCP SYN 封包的臨界值超過定義數值，Vigor 路由器在所設定之逾時期間即開始捨棄其後之 TCP SYN 封包，這項功能的目的是防止 TCP SYN 封包嚐試耗盡路由器有限的資源。臨界值和逾時的預設值分別爲每秒 50 個封包和 10 秒。 |
| **啓用 UDP flood 攻擊防禦功能** | 勾選此項以啓動 UDP 攻擊防禦功能， 一旦檢查到 UDP 封包臨界值超過定義數值，Vigor 路由器在所設定之逾時期間即開始捨棄其後之 UDP 封包。臨界值和逾時的預設值分別爲每秒 150 個封包和 10 秒。 |
| **啓用 ICMP Fragment 封包** | 勾選此項以啓動 ICMP Fragment 封包，與 UDP 攻擊防禦功能相同的是，一旦檢查到 ICMP 封包臨界值超過定義數值，路由器便會於所設定之逾時期間，不再回應來自網際網路的 ICMP 需求。臨界值和逾時的預設值分別爲每秒 50 個封包和 10 秒。 |
| **啓用防禦通訊埠掃瞄偵測功能** | 通訊埠掃瞄藉由傳送大量封包到數個通訊埠，以嘗試找出未知服務所回應之內容來攻擊 Vigor 路由器。勾選此方塊啓動通訊埠掃瞄檢測功能，當利用通訊埠掃瞄臨界值速率而檢測出惡意探測之行爲時，Vigor 路由器將傳送警告訊息出去。臨界值的 |

預設值爲每秒 150 個封包。

**封鎖 IP options** 勾選此項以啓動阻攔 IP options 功能，Vigor 路由器將會忽略資料封包頭中(含 IP 選項區)的 IP 封包。限制的原因是 IP option 的出現是區域網路安全性中的弱點，因爲它攜帶令人注意的資訊像是安全性、TCC (封閉使用者群組)參數、網際網路位址、路由訊息等等，讓外部的竊聽者有機會取得您虛擬網路的細節內容。

**封鎖 Land 攻擊** 勾選此項以強迫 Vigor 路由器防護 Land 攻擊，Land 攻擊結合含 IP spoofing 的 SYN 攻擊技術，當駭客傳送 spoofed SYN 封包(連同相同來源和目的位址)，以及通訊埠號至受害一方時，Land 攻擊即由此發生。

**封鎖 Smurf 攻擊** 勾選此項以啓動封鎖 Smurf 攻擊功能，Vigor 路由器將忽略任何一次的播送 ICMP 回應需求。

**封鎖路由追蹤** 勾選此項以強迫 Vigor 路由器不轉送任何路由封包的行蹤。

**封鎖 SYN Fragment 封包** 勾選此項以啓動封鎖 SYN Fragment 的封包功能。Vigor 路由器將會停止任何具有 SYN 旗標及更多的區段設定之封包傳送作業。

**封鎖 Fraggle 攻擊** 勾選此項以啓動封鎖 Fraggle 攻擊功能，任何播送來自網際網路的 UDP 封包都會被封鎖起來。
啓動 DoS/DDoS 防禦功能可能會阻擋一些合法的封包，例如當您啓動 fraggle 攻擊防禦時，所有來自網際網路的 UDP 封包播送都會被阻擋在外，因此得自網際網路的 RIP 封包全都會被阻擋掉。

**封鎖 TCP Flags scan** 勾選此項以啓動阻攔 TCP Flags 掃描功能，任何具有異常 TCP 封包的設定都會被捨棄掉，這些掃描行動包含有 *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* 以及 *full Xmas scan* 等等。

**封鎖 Tear Drop 攻擊** 勾選此項以啓動封鎖 Tear Drop 攻擊功能，很多機器在接收到超過最大値得 ICMP 資料段(封包)時，系統就會當機。爲了避免這類型的攻擊行爲，Vigor 路由器便被設計成具有捨棄片段 ICMP (超過 1024 位元組)封包的能力。

**封鎖 Ping of Death 攻擊** 勾選此項以啓動封鎖 Ping of Death 攻擊功能，這項攻擊意味著犯罪者傳送重疊封包至目的主機，這些目的主機一旦重新建構封包時就會造成當機現象，Vigor 路由器將會阻擋此種攻擊活動的封包進入。

**封鎖 ICMP 封包片段攻擊** 勾選此項以啓動封鎖 ICMP 封包片段功能，任何含有多個片段的 ICMP 封包都會被捨棄阻擋。

**封鎖不明封包協定封包** 勾選此項以啓動封鎖不明封包協定封包功能，個別 IP 封包在資料段封包頭中都擁有一個協定區域，指名該協定於上層運作的類型。

**警告訊息** 我們提供使用者系統記錄功能以便檢視路由器發出的訊息。作爲系統紀錄伺服器，使用者可接收來自路由器(系統紀錄用戶端)傳送之報告。

所有與 DoS 攻擊有關的警告訊息都將傳送與使用者，使用者可以重新檢查其內容，在訊息中尋找關鍵字，所遭受的任何攻擊之名稱即可立即檢測出來。

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

| SysLog Access Setup | | Mail Alert Setup | |
|---|---|---|---|
| ☑ Enable | | ☑ Enable | Send a test e-mail |
| Server IP Address | 192.168.1.5 | SMTP Server | |
| Destination Port | 514 | Mail To | |
| Enable syslog message: | | Return-Path | |
| ☑ Firewall Log | | ☐ Authentication | |
| ☑ VPN Log | | User Name | |
| ☑ User Access Log | | Password | |
| ☑ Call Log | | Enable E-Mail Alert: | |
| ☑ WAN Log | | ☑ DoS Attack | |
| ☑ Router/DSL information | | ☑ IM-P2P | |

OK Clear Cancel

DrayTek Syslog 3.7.0

Controls: 192.168.1.1 — Vigor Series

LAN Status: TX Packets 4175, RX Packets 3668

WAN Status: Gateway IP (Fixed) 172.16.3.4, TX Packets 343, TX Rate 3; WAN IP (Fixed) 172.16.3.229, RX Packets 2558, RX Rate 126

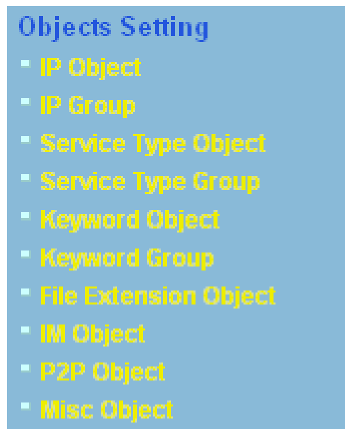
Firewall Log | VPN Log | User Access Log | Call Log | WAN Log | Others | Network Information | Net State | Traffic Graph

| Time | Host | Message |
|---|---|---|
| Jan 1 00:00:42 | Vigor | DoS syn_flood Block(10s) 192.168.1.115,10605 -> 192.168.1.1,23 PR 6(tcp) len 20 40 -S 394375 |
| Jan 1 00:00:34 | Vigor | DoS icmp_flood Block(10s) 192.168.1.115 -> 192.168.1.1 PR 1(icmp) len 20 60 icmp 0/8 |

ADSL Status: Mode, State, Up Speed, Down Speed, SNR Margin, Loop Att

# 4.6 物件和群組

對某些範圍內的 IP 和侷限於特定區域的服務通訊埠，通常可以套用於路由器網頁設定中。因此我們可以將他們定義成為物件，並結合成群組以便後續能方便的應用。之後，我們可以選擇該物件/群組來套用，比方說，相同部門內所有的 IP 可定義成為一個 IP 物件(意即 IP 位址範圍)。




## 4.6.1 IP 物件

您可設定 192 組不同條件的 IP 物件。

Objects Setting >> IP Object

IP Object Profiles: | Set to Factory Default |

| Index | Name | Index | Name |
|---|---|---|---|
| 1. | | 17. | |
| 2. | | 18. | |
| 3. | | 19. | |
| 4. | | 20. | |
| 5. | | 21. | |
| 6. | | 22. | |
| 7. | | 23. | |
| 8. | | 24. | |
| 9. | | 25. | |
| 10. | | 26. | |
| 11. | | 27. | |
| 12. | | 28. | |
| 13. | | 29. | |
| 14. | | 30. | |
| 15. | | 31. | |
| 16. | | 32. | |

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 >>　　Next >>

**回復出廠預設值**　　清除全部的設定資料。

按下任一索引號碼進入下述畫面：

Objects Setting >> IP Object

Profile Index : 1

| | |
|---|---|
| Name: | RD Department |
| Interface: | Any |
| Address Type: | Range Address |
| Start IP Address: | 192.168.1.64 |
| End IP Address: | 192.168.1.75 |
| Subnet Mask: | 0.0.0.0 |
| Invert Selection: | ☐ |

OK Clear Cancel

**名稱** 請輸入本設定檔的名稱，最多可以輸入 15 個字元。

**介面** 請選擇適當的介面(WAN, LAN 或是任何一種)。

Interface: Any

Any
LAN
WAN

例如，**編輯過濾器規則**中的**方向**設定會要求您針對 WAN 或 LAN 介面指定一個 IP 或是 IP 範圍，或是任何的 IP 位址，如果您選擇 LAN 作爲介面，並選擇 LAN 作爲**編輯過濾器規則**中的**方向**設定，那麼所有的 LAN 介面的 IP 位址通通都會開放予您在**編輯過濾器規則**頁面上選擇。

**位址類型** 決定 IP 位址的位址類型。
如果物件僅包含 IP 位址的話，請選擇**單一位址**。
如果物件包含某個範圍內數個 IP 位址的話，請選擇**範圍位址**。
如果物件包含 IP 位址的子網路的話，請選擇**子網路位址**。
如果物件包含任何一種 IP 位址的話請選擇**任何位址**。

**起始 IP 位址** 輸入單一位址類型所需的起始 IP 位址。

**結束 IP 位址** 如果選擇的是範圍位址類型，請輸入結束 IP 位址。

**子網路位址** 如果選擇的是**子網路位址**類型，請輸入子網路遮罩位址。

**反向選擇** 如果勾選此項的話，除了上面所提及的以外，其他的 IP 位址將會在被選擇之後全部套用上設定內容。

下表爲 IP 物件設定的範例之一。

Objects Setting >> IP Object

IP Object Profiles:

| Index | Name |
|---|---|
| 1. | RD Department |
| 2. | Finanical Dept. |
| 3. | HR Department |
| 4. | |

### 4.5.2 IP 群組

本頁可讓您綁定數個 IP 物件成為一個 IP 群組。

Objects Setting >> IP Group

IP Group Table: | Set to Factory Default |

| Index | Name | Index | Name |
|---|---|---|---|
| 1. | | 17. | |
| 2. | | 18. | |
| 3. | | 19. | |
| 4. | | 20. | |
| 5. | | 21. | |
| 6. | | 22. | |
| 7. | | 23. | |
| 8. | | 24. | |
| 9. | | 25. | |
| 10. | | 26. | |
| 11. | | 27. | |
| 12. | | 28. | |
| 13. | | 29. | |
| 14. | | 30. | |
| 15. | | 31. | |
| 16. | | 32. | |

**回復出廠預設值** 清除全部的設定資料。

按下任一索引號碼以便完成詳細設定。

Objects Setting >> IP Group

Profile Index : 1

Name:

Interface: Any

Available IP Objects

1-RD Department
2-Finanical Dept.
3-HR Department

>>
<<

Selected IP Objects

OK Clear Cancel

| | |
|---|---|
| **名稱** | 請輸入本設定檔的名稱，最多可以輸入 15 個字元。 |
| **介面** | 請選擇適當的介面(WAN, LAN 或是任何一種)以顯示所有指定介面內的 IP 物件。 |
| **可用之 IP 物件** | 所有選定之指定介面中可用的 IP 物件全都會顯示在此方塊中。 |
| **選定 IP 物件** | 按下 **>>** 按鈕來新增選定 IP 物件並呈現在此方塊內。 |

### 4.6.3 服務類型物件

您可設定 96 組不同條件的服務類型物件。

Objects Setting >> Service Type Object

Service Type Object Profiles: | Set to Factory Default |

| Index | Name | Index | Name |
|---|---|---|---|
| 1. | | 17. | |
| 2. | | 18. | |
| 3. | | 19. | |
| 4. | | 20. | |
| 5. | | 21. | |
| 6. | | 22. | |
| 7. | | 23. | |
| 8. | | 24. | |
| 9. | | 25. | |
| 10. | | 26. | |
| 11. | | 27. | |
| 12. | | 28. | |
| 13. | | 29. | |
| 14. | | 30. | |
| 15. | | 31. | |
| 16. | | 32. | |

<< 1-32 | 33-64 | 65-96 >> Next >>

**回復出廠預設值** 清除全部的設定資料。

按下任一索引號碼進入下述畫面：

Objects Setting >> Service Type Object Setup

Profile Index : 1

| | |
|---|---|
| Name | www |
| Protocol | TCP 6 |
| Source Port | = 1 ~ 65535 |
| Destination Port | = 1 ~ 65535 |

OK Clear Cancel

**名稱** 輸入此設定檔的名稱。

**介面** 請選擇此設定檔所要套用的適當介面。

TCP 6

Any
ICMP
IGMP
TCP
UDP
TCP/UDP
Other

**來源/目標通訊埠** **來源通訊埠**與**目標通訊埠**欄位皆為 TCP/UDP 可用之通訊埠，如果是其他的通訊協定，這些欄位即可省略，過濾器規

則將可過濾任何一種通訊埠號。
**(=)** – 當第一與最後的數值相同時，此符號表示一個通訊埠。當第一與最後的數值不同時，此符號表示此設定檔所適用的通訊埠號範圍。
**(!=)** –當第一與最後的數值相同時，此符號表示除了這裡所指明的通訊埠以外，全都適用於此設定檔。當第一與最後的數值不同時，此符號表示所有的通訊埠除了此處所設定的範圍以外，全都適用於此設定檔。
**(>)** – 大於此數值的通訊埠號皆可使用。
**(<)** – 小於此數值的通訊埠號皆可使用。

下表為服務類型物件設定的範例之一。

Objects Setting >> Service Type Object

Service Type Object Profiles:

| Index | Name |
|---|---|
| 1. | SIP |
| 2. | RTP |
| 3. | |

### 4.5.4 服務類型群組

本頁可讓您綁定數個服務類型物件成為一個群組。

Objects Setting >> Service Type Group

Service Type Group Table: | Set to Factory Default |

| Group | Name | Group | Name |
|---|---|---|---|
| 1. | | 17. | |
| 2. | | 18. | |
| 3. | | 19. | |
| 4. | | 20. | |
| 5. | | 21. | |
| 6. | | 22. | |
| 7. | | 23. | |
| 8. | | 24. | |
| 9. | | 25. | |
| 10. | | 26. | |
| 11. | | 27. | |
| 12. | | 28. | |
| 13. | | 29. | |
| 14. | | 30. | |
| 15. | | 31. | |
| 16. | | 32. | |

**回復出廠預設值** 清除全部的設定資料。

按下任一索引號碼進入下述畫面：

Objects Setting >> Service Type Group Setup

Profile Index : 1

Name: VoIP

Available Service Type Objects

1-SIP
2-RTP

Selected Service Type Objects

»
«

OK Clear Cancel

| | |
|---|---|
| **名稱** | 輸入此設定檔名稱。 |
| **可用之服務類型物件** | 您可以從 IP 物件頁面中先新增一些服務類型，所有可用的服務類型將會顯示在此區域中。 |
| **選定之服務類型物件** | 按下 **>>** 按鈕來新增選定服務類型並呈現在此方塊內。 |
| **回復出廠預設值** | 清除全部的設定資料。 |

按下任一索引號碼進入下述畫面：

# 4.7 CSM 設定檔

### 數位內容安全管理(Content Security Management, CSM)

### IM/P2P 過濾器

由於即時通訊應用程式蓬勃的發展，人與人間的通訊變得越來越容易。然而一些企業利用此種程式作爲與客戶通訊的有力工具時，部分公司對此可能還是抱持保留態度，這是因爲他們想要減少員工在上班時間誤用此程式或是防止未知的安全漏洞發生。對於準備應用點對點程式的公司來說，情況也是相同的，因爲檔案分享可以很方便但是同時也很危險。爲了應付這些需求，我們提供了 CSM 阻擋功能。

### 內容過濾器

爲了提供一個適當的網路空間給予使用者，Vigor 路由器配有 URL 內容過濾器，可限制一些不合法的資料於網站上進出，同時也禁止隱藏惡意碼的網路特徵於路由器內出入。

一旦使用者輸入關鍵字連結，URL 關鍵字阻擋工具將會拒絕該網頁之 HTTP 需求，如此一來使用者即無法存取該網站。您可以這樣想像一下，URL 內容過濾器爲一個訓練有素的便利商店櫃員，絕對不販售成人雜誌給予未成年的小孩子。在辦公室內，URL 內容過濾器也可以提供與工作相關的環境，由此來增加員工的工作效率。URL 內容過濾器爲什麼可以比傳統防火牆在過濾方面提供更好的服務呢？那是因爲它能夠檢查 URL 字串或是一些隱藏在 TCP 封包負載的 HTTP 資料，而一般防火牆僅能以 TCP/IP 封包標頭來檢測封包。

換言之，Vigor 路由器可以防止使用者意外自網頁下載惡意的程式碼。惡意碼隱藏在執行物件當中是一件很普遍的事情，像是 ActiveX、Java Applet、壓縮檔和其他執行檔案。一旦用戶下載這些類型的檔案，用戶便會有這些可能爲系統帶來威脅的風險，例如一個 ActiveX 控制物件通常用於提供網頁人機通信交換功能，萬一裡面隱藏惡意的程式碼的話，該程式碼就可能會佔據使用者的系統。

### 網頁內容過濾器

我們都知道網際網路上的內容，有時候可能並不太合宜，作爲一個負責任的父母或是雇主，您應該保護那些您信賴的人免受危險的侵擾。藉由 Vigor 路由器的網頁過濾服務，您可以保護您的商業機密不受一般常見威脅；對於父母來說，您可以保護您的孩童不致誤闖成人網站或是成人聊天室。

一旦您啓動了網頁內容過濾服務，也選擇一些您想要限制存取的網站目錄，每個 URL 位址需求(例 www.bbc.co.uk) 將在由 SurfControl 所運作的伺服器資料庫中先接受檢測。資料庫涵蓋 70 種語言和 200 個國家，超過 1 億個網頁，區分成 40 種容易瞭解的目錄。此資料庫每一天都由網際網路的國際研究團隊不斷更新，伺服器將查閱 URL 然後傳回其類別給路由器，您的 Vigor 路由器即可按照您所選擇的分類項目來決定是否允許用戶存取該網站，因爲每一個多路負載平衡資料庫伺服器一次可以管理數百萬的分類需求。

CSM
- IM/P2P Filter Profile
- URL Content Filter Profile
- Web Content Filter Profile

## 4.8 頻寬管理

下面是頻寬管理的設定項目:




### 4.8.1 NAT 連線數限制

擁有虛擬 IP 的電腦可以透過 NAT 路由器存取網際網路，針對此連線需求路由器將會產生 NAT 連線數的紀錄，P2P (Peer to Peer)應用程式(如 BitTorren)經常需要很大的連線數來處理，同時也會佔據很大的資源空間，造成重要的資料存取動作受到嚴重的影響。為了解決這種問題，您可以使用連線數限制來限制指定主機的連線數

在**頻寬管理**群組中，按**連線數限制**開啓如下的網頁。

Bandwidth Management >> Sessions Limit

Sessions Limit

Enable Disable

Default Max Sessions: 100

Limitation List

| Index | Start IP | End IP | Max Sessions |
|---|---|---|---|

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Add Edit Delete

Time Schedule

Index(1-15) in Schedule Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

OK

如果要啓動限制連線數的功能，只要在此頁面上按**啓用**鈕，並設定預設的連線數限制即可。

| | |
|---|---|
| **啓用** | 按此鈕啓動連線數限制功能。 |
| **停用** | 按此鈕關閉連線數限制功能。 |
| **預設最大連線數** | 定義區域網路中每台電腦的預設連線數。 |
| **限制清單** | 顯示網頁中所設定的指定限制之電腦清單資料。 |
| **起始 IP** | 定義連線數限制的起始 IP 位址。 |
| **結束 IP** | 定義連線數限制的結束 IP 位址。 |

| | |
|---|---|
| **最大連線數** | 定義指定 IP 位址的範圍中可用的連線數，如果您沒有在此區設定連線數，系統將會使用此機種所支援之預設連線數 (10000)。 |
| **新增** | 新增指定連線數限制並顯示在上面的框框中。 |
| **編輯** | 允許您編輯選定的連線數設定。 |
| **刪除** | 刪除限制清單上任何一個您所選定的設定。 |
| **索引號碼(1-15)於排程設定..** | 您可以輸入四組時間排程，所有的排程都可在**應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。 |

## 4.8.2 頻寬限制

從 FTP,HTTP 或是某些 P2P 應用程式的下行或上行資料會佔據很大的頻寬，並影響其他程式的運作。請使用限制頻寬讓頻寬的應用更有效率。

在**頻寬管理**群組中，按**頻寬限制**開啟如下的網頁。

Bandwidth Management >> Bandwidth Limit

Bandwidth Limit

○ Enable ☐ Apply to 2nd Subnet ⦿ Disable

Default TX Limit: 200 Kbps Default RX Limit: 800 Kbps

Limitation List

| Index | Start IP | End IP | TX limit | RX limit |
|---|---|---|---|---|

Specific Limitation

Start IP: End IP:

TX Limit: Kbps RX Limit: Kbps

Add Edit Delete

Time Schedule

Index(1-15) in Schedule Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

OK

如果要啟動限制頻寬的功能，只要在此頁面上按**啟用**鈕，並設定預設的上下行資料傳送限制即可。

| | |
|---|---|
| **啟用** | 按此鈕啟動限制頻寬功能。. |
| **停用** | 按此鈕關閉限制頻寬功能。 |
| **預設傳送限制** | 定義區域網路中每台電腦預設的上行速度。 |
| **預設接收限制** | 定義區域網路中每台電腦預設的下行速度。 |

| | |
|---|---|
| **限制清單** | 顯示網頁中所設定的指定限制之電腦清單資料。 |
| **起始 IP** | 定義限制頻寬的起始 IP 位址。 |
| **結束 IP** | 定義限制頻寬的結束 IP 位址。 |
| **傳送限制** | 定義上行傳送的速度限制，如果您未在此區設定限制的話，系統將使用您在每個索引內容中索引中所預設的限制速度。 |
| **接收限制** | 定義下行傳送的速度限制，如果您未在此區設定限制的話，系統將使用您在每個索引內容中索引中所預設的限制速度。 |
| **新增** | 新增指定速度限制並顯示在上面的框框中。 |
| **編輯** | 允許您編輯選定的限制設定。 |
| **刪除** | 刪除限制清單上任何一個您所選定的設定。 |
| **索引號碼(1-15)於排程設定..** | 您可以輸入四組時間排程，所有的排程都可在**應用-排程**網頁上事先設定完畢，然後在此輸入該排程的對應索引號碼即可。 |

## 4.8.3 服務品質(QoS)

QoS (Quality of Service)管理部署可確保所有應用程式能夠接收到所需的服務以及足夠的頻寬，符合用戶所期待的效果，此項控制對現代企業網路來說是相當重要的觀點。

使用 QoS 的理由之一是很多 TCP 為主的應用程式嘗試不斷增加其傳輸速率，導致消耗掉全部的頻寬，我們稱之為 TCP 慢速啓動。如果其他的應用程式未受 QoS 的保護，那麼他們在擁擠的網路中將會降低效能，對那些無法忍受任何損失、延遲的功能像是 VoIP、視訊會議以及流動影像來說，這項控制尤其必要。

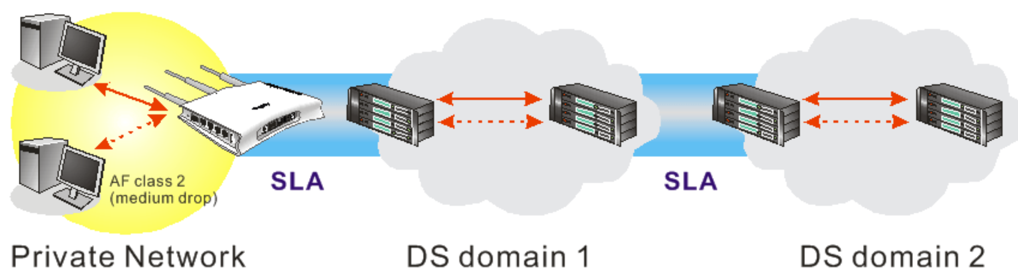
另一個理由是由於網路的擁擠狀況，內部連線迴路速度不符合或是傳輸流量過份聚集，資料封包排隊等候傳送，整個傳輸慢了下來。如果沒有定義後先後順序，以指定在滿檔的隊伍中哪個封包必須丟棄，上述提及的應用程式封包就可能成為被捨棄掉的一個，這樣的話對應用程式的成效會造成令人無法想像的後果。

在基本設定中有二個元件要注意：

- 分類: 可辨識低潛在因素或是重要的應用程式，並標示這些程式為高優先權服務等級，以便在網路中能夠強迫執行。
- 排定計畫: 以服務等級分類為基礎來指定封包排列順序以及整合的服務型態。

基本 QoS 應用是以 IP 封包頭中之服務類型資訊為基礎來分類及規劃封包，例如為了確保封包頭之連線，電信工作人員在執行大量運作時，可能會強迫一個 QoS 控制索引保留頻寬予 HTTP 連線。

Vigor 路由器作為 DS 管理之終端路由器，應該檢查通過流量之 IP 封包頭中標記 DSCP 之數值，這樣才可分配特定資源數量來執行適當政策、分類或是排程。網路骨幹之核心路由器在執行動作前也會做同樣的檢查，以確保整個 QoS 啓動之網路中服務等級保持一致性。




QoS 將以上傳/下載速度比率來定義，我們也會提供一些 QoS 需求應用給您參考，設定數値會依照網路實際狀況而有所改變。

在**頻寬管理**群組中，選擇**服務品質**開啓如下的網頁。

Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

| Status | Bandwidth | Directon | Class 1 | Class 2 | Class 3 | Others | UDP Bandwidth Control | |
|---|---|---|---|---|---|---|---|---|
| Enable | 10000Kbps/10000Kbps | Outbound | 25% | 25% | 25% | 25% | Inactive | Setup |

Class Rule

| Index | Name | Rule | Service Type |
|---|---|---|---|
| Class 1 | | Edit | Edit |
| Class 2 | | Edit | |
| Class 3 | | Edit | |

本頁顯示 WAN 介面上的 QoS 設定成果，按下設定連結進入下一層頁面，至於類別規則，則按下該頁面上的**編輯**按鈕進入另一層畫面來設定即可。

您可以設定 WAN 介面的一般設定，並視您的需要來編輯類別規則並且編輯類別規則的服務類型。

## WAN 基本設定

當您按下設定時，您可調整 WAN 介面的 QoS 頻寬比率，系統提供您四種類別作爲 QoS 控制之用，前三種(類別 1 到類別 3)可視您的需求來調整，而最後一個則保留給那些不符合上面定義之規則等封包使用。

Bandwidth Management >> Quality of Service

General Setup

☑ Enable the QoS Control [OUT]

| | | |
|---|---|---|
| WAN Inbound Bandwidth | 10000 | Kbps |
| WAN Outbound Bandwidth | 10000 | Kbps |

| Index | Class Name | Reserved_bandwidth Ratio |
|---|---|---|
| Class 1 | | 25 % |
| Class 2 | | 25 % |
| Class 3 | | 25 % |
| | Others | 25 % |

☐ Enable UDP Bandwidth Control — Limited_bandwidth Ratio 25 %

☐ Outbound TCP ACK Prioritize — Online Statistics

[OK] [Clear] [Cancel]

**啓用服務品質(QoS)控制..** 預設狀態下，這個功能是啓用的。
請同時定義 QoS 控制設應所應用的流量方向。
**下載-** 僅適用於進入的封包。
**上傳-** 僅適用於輸出的封包。
**雙向-** 適用於進入與輸出的封包。
勾選此方塊並按下**確定**，**連線狀態統計**連結即可出現在此頁面上。

**WAN 下載頻寬** 允許您設定 WAN 資料輸入的連線速度。預設值為 10000kbps。

**WAN 上傳頻寬** 允許您設定 WAN 資料輸入的連線速度。預設值為 10000kbps。

例如，您的 ADSL 支援 1M 的下行與 256K 上行速度，請將 **WAN 下載頻寬** 設定為 1000kbps 而 **WAN 上傳頻寬** 設定為 256kbps。

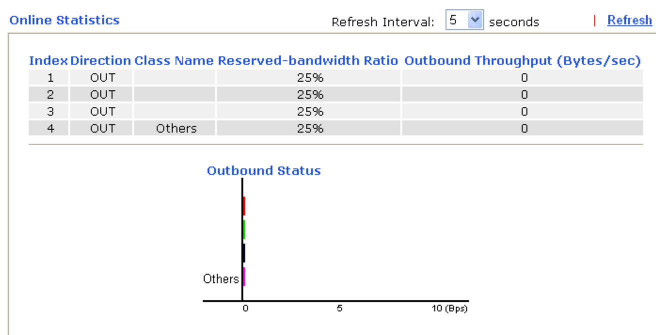
**保留頻寬比例** 保留作為群組索引所可應用的比率。

**啓用 UDP 頻寬控制** 勾選此設定並在右邊設定限制的頻寬比率，這是 TCP 應用的一種保護機制，因為 UDP 應用程式會消耗很多的頻寬。

**優先處理對外 TCP ACK** 下載和上傳之的頻寬在 ADSL2+ 環境中差異是很大的，因為下載速度可能會受到上傳 TCP ACK 的影響，您可以勾選此方塊讓 ACK 上傳得快一點，以便讓網路流通的更順暢。

**限制頻寬比率** 此處所輸入的比率保留作為 UDP 應用之需。

**連線狀態統計** 顯示服務品質的連線狀態統計圖供使用者參考。




## 編輯 Qos 的類別規則

前三種(類別 1 到類別 3)可視您的需求來調整，編輯或是刪除類別規則，請按該項類別的索引連結即可。

Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

| Status | Bandwidth | Directon | Class 1 | Class 2 | Class 3 | Others | UDP Bandwidth Control | |
|---|---|---|---|---|---|---|---|---|
| Enable | 10000Kbps/10000Kbps | Outbound | 25% | 25% | 25% | 25% | Inactive | Setup |

Class Rule

| Index | Name | Rule | Service Type |
|---|---|---|---|
| Class 1 | | Edit | |
| Class 2 | | Edit | Edit |
| Class 3 | | Edit | |

在您按下索引連結之後，您可以看到如下的頁面。現在您可以定義該類別的名稱，在本例中，TEST 用來作爲類別索引 1 的名稱。

Bandwidth Management >> Quality of Service

Class Index #1

Name: Test

| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
| --- | --- | --- | --- | --- | --- |
| 1 | Empty | - | - | - | - |

Add Edit Delete

OK Cancel

若要新增一個新的規則，請按**新增**開啓下列畫面。

Bandwidth Management >> Quality of Service

Rule Edit

ACT

Local Address: Any [Edit]

Remote Address: Any [Edit]

DiffServ CodePoint: ANY

Service Type: ANY

Note: Please choose/setup the Service Type first.

OK Cancel

**啓用** 勾選此方塊啓用本頁的設定。

**本機位址** 按**編輯**按鈕以設定規則的來源位址。

**遠端位址** 按**編輯**按鈕以設定規則的目標位址。

**編輯** 讓您編輯來源/目標位址資訊。

http://192.168.1.1/doc/QosIpEdt.htm - Microsoft Internet Explorer

Address Type: Subnet Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

OK Close

**位址類型** – 決定來源位址的位址類型。
關於**單一位址**，您可以填入起始 IP 位址。
關於**範圍位址**，您必須填入起始和終點 IP 位址。
關於**子網路位址**，您必須填入起始 IP 位址和子網路遮罩。

**DiffServ CodePoint** 所有的資料封包將會被切割成不同等級，並且依照系統的等級層別來處理資料封包。請指定資料所需的層級作為 DoS 控制之用。

**服務類型** 決定 QoS 控制處理時資料的服務類型，這項類型可以視情況編輯改變，您可以從下拉式選項中選擇事先定義的服務類型，這些類型都是出廠時即設定好的類型，請自行挑選一種想要使用的類型。

另外，您可以為一種類別指定 20 組規則，如果您想要編輯現存的規則，請點選該項按鈕，然後按下**編輯**鈕開啓編輯視窗以修正該規則。

Bandwidth Management >> Quality of Service

Class Index #1

Name Test

| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
|---|---|---|---|---|---|
| 1 ⦿ | Active | Any | Any | IP precedence 2 | TFTP(UDP:69) |

Add Edit Delete

OK Cancel

## 編輯類別規則的服務類型

要新增、編輯或刪除服務類型，請按服務類型區域下方的**編輯**連結。

Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

| Status | Bandwidth | Directon | Class 1 | Class 2 | Class 3 | Others | UDP Bandwidth Control | |
|---|---|---|---|---|---|---|---|---|
| Enable | 10000Kbps/10000Kbps | Outbound | 25% | 25% | 25% | 25% | Inactive | Setup |

Class Rule

| Index | Name | Rule | Service Type |
|---|---|---|---|
| Class 1 | | Edit | |
| Class 2 | | Edit | Edit |
| Class 3 | | Edit | |

在您按下**編輯**按鈕之後，下面的畫面將會出現。

**Bandwidth Management >> Quality of Service**

**User Defined Service Type**

| NO | Name | Protocol | Port |
|---|---|---|---|
| 1 | Empty | - | - |

Add　Edit　Delete

Cancel

新增一個規則請按下**新增**按鈕開啓設定頁面，如果您想要編輯現有的服務類型，請選擇該項並按下**編輯**連結開啓如下頁面：

**Bandwidth Management >> Quality of Service**

**Service Type Edit**

| | |
|---|---|
| Service Name | |
| Service Type | TCP　6 |
| Port Configuration | |
| Type | Single　Range |
| Port Number | 0 - 0 |

OK　Cancel

| | |
|---|---|
| **服務名稱** | 輸入新的服務名稱。 |
| **服務類型** | 請選擇新服務所需的類型(TCP, UDP or TCP/UDP)。 |
| **通訊埠設定** | 按**單一**或是**範圍**，如果您選擇的是範圍，您必須輸入起始通訊埠號和結束通訊埠號。<br>**通訊埠號** –如果您選擇範圍爲服務類型，請在此輸入起始和結束通訊埠號。 |

另外，您可以指定 40 組服務類型，如果您想要編輯或是刪除現存的服務類型，請點選該項按鈕，然後按下**編輯**鈕開啓編輯視窗以修正該服務類型。

## 4.9 其他應用

下圖顯示**應用**的功能項目：




### 4.9.1 Dynamic DNS

### 動態 DNS

當您透過 ISP 業者嘗試連接到網際網路時，ISP 業者提供的經常是一個浮動 IP 位址，這表示指派給您的路由器使用之真實 IP 位址每次都會有所不同，DDNS 可讓您指派一個網域名稱給予浮動廣域網路 IP 位址。它允許路由器線上更新廣域網路 IP 位址，以便對應至特定的 DDNS 伺服器上。一旦路由器連上網路，您將能夠使用註冊的網域名稱，並利用網際網路存取路由器或是內部虛擬的伺服器資料。如果您的主機擁有網路伺服器、FTP 伺服器或是其他路由器後方提供的伺服器，這項設定就特別有幫助也有意義。

在您使用 DDNS 時，您必須先向 DDNS 服務供應商要求免費的 DDNS 服務，路由器提供分別來自不同 DDNS 服務供應商的三種帳號。基本上，Vigor 路由器和大多數的 DDNS 服務供應商 **www.dyndns.org, www.no-ip.com**、**www.dtdns.com**、**www.changeip.com**、**www.dynamic-nameserver.com** 像是都能相容，您應該先造訪其網站為您的路由器註冊自己的網域名稱。

**啟動此功能並增加一個動態 DNS 帳戶**

1. 假設您已經從 DDNS 供應商註冊了一個網域名稱(例如 hostname.dyndns.org)，且獲得一個帳號，其使用者名稱為 *test*；密碼為: *test*。
2. 自**應用**群組選擇**動態 DNS** 設定，下述頁面即會出現在螢幕上。

Applications >> Dynamic DNS Setup

Dynamic DNS Setup | Set to Factory Default |

☑ Enable Dynamic DNS Setup [View Log] [Force Update]

Auto-Update interval 1440 Min(s)

Accounts:

| Index | Domain Name | Active |
| --- | --- | --- |
| 1. | . | x |
| 2. | . | x |
| 3. | . | x |

[OK] [Clear All]

| | |
| --- | --- |
| **回復出廠預設值** | 清除全部設定資料並回復到出廠的設定。 |
| **啓用動態 DNS 設定** | 勾選此方塊啓用此功能。 |
| **索引** | 按下方的號碼連結進入 DDNS 設定頁面，以設定帳戶。 |

**網域名稱** 顯示您在 DDNS 設定頁面上所設定的網域名稱。

**啓用** 顯示此帳號目前是啓用或是停用狀態。

**檢視記錄** 可開啓另一個對話盒並顯示 DDNS 資訊紀錄。

**強迫更新** 按此按鈕強迫路由器取得最新的 DNS 資訊。

3. 選擇索引號碼 1，爲您的路由器新增一個帳號。勾選**啓用動態 DNS 帳號**，然後選擇正確的服務供應商(例 dyndns.org)，輸入註冊的主機名稱(例 hostname)，並於網域名稱區塊中輸入網域的字尾名稱(例 dyndns.org)；接著輸入您的帳號登入名稱(例 dray)和密碼(例 test)。

Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup

Index : 1

☑ Enable Dynamic DNS Account

| | |
|---|---|
| Service Provider | dyndns.org (www.dyndns.org) |
| Service Type | Dynamic |
| Domain Name | chronic6683 . dyndns.org  dyndns.org |
| Login Name | chronic6683 (max. 64 characters) |
| Password | ●●●●●●●●●●●● (max. 23 characters) |
| ☐ Wildcards | |
| ☐ Backup MX | |
| Mail Extender | |

OK Clear Cancel

**啓用動態 DNS 帳號** 勾選此方塊以啓用目前帳號，如果您勾選此方塊，您可在步驟 2 中的網頁上看到啓動欄位出現勾選標示。

**WAN 介面** 選擇適合的介面以套用相關設定。

**服務供應商** 爲此 DDNS 帳號選擇適當的服務供應商。

**服務類型** 選擇服務類型(動態、自訂、固定)。如果您選擇的是**自訂**，您可以修正網域名稱區域中所選定的網域資料。

**網域名稱** 輸入您所申請的網域名稱。請使用下拉式選項選擇想要使用的一個名稱。

**登入名稱** 輸入您在申請網域名稱時所設定之登入名稱。

**密碼** 輸入您在申請網域名稱時所設定之密碼。

**郵件延伸程式** 某些 DDNS 伺服器可能會要求提供額外的資訊，如電子郵件地址，請您在此輸入必要的電子郵件地址，以配合該 DDNS 伺服器之需要。

5. 按**確定**按鈕啓動此設定，您將會看到所做的設定已被儲存。

**萬用字元**與**備份 MX** 並非所有的動態 DNS 服務商都有支援，有關此部分內容，請您自服務商的網站上取得更詳盡的資訊。

**關閉此功能並清除全部動態 DNS 帳號**

取消勾選**啓用動態 DNS 帳號**，並按下**清除全部**按鈕停用此功能以及清除路由器內所有的帳號。

**刪除動態 DNS 帳號**

在**動態 DNS 設定**頁面上，請按您想要刪除之帳號的索引號碼，然後按**清除全部**按鈕即可刪除該帳號。

## 4.9.2 排程

Vigor 路由器可允許您手動更新，或利用網路時間協定(NTP)更新時間，因此您不只可以規劃路由器在特定時間撥號至網際網路，也能限制於特定時間內存取網際網路資料，如此一來使用者只能在限定時間(或說上班時間)上網，時間排程也可以和其他功能搭配使用。

您必須在設定排程前先設定好時間，在**系統維護**群組中，選擇**時間和日期**以開啓時間設定頁面，按**取得時間**按鈕取得與電腦(或網際網路)一致的時間，一旦您關閉或是重新啓動路由器，時鐘的時間也會重新啓動。還有另一種方法可以設定時間，您可以在網際網路上請求 NTP 伺服器(這是一個時間伺服器)以同步化路由器的時鐘，這個方法只能在廣域網路連線建立時才能使用。

Applications >> Schedule

Schedule: | Set to Factory Default |

| Index | Status | Index | Status |
|---|---|---|---|
| 1. | x | 9. | x |
| 2. | x | 10. | x |
| 3. | x | 11. | x |
| 4. | x | 12. | x |
| 5. | x | 13. | x |
| 6. | x | 14. | x |
| 7. | x | 15. | x |
| 8. | x | | |

Status: v --- Active, x --- Inactive

| | |
|---|---|
| **回復出廠預設值** | 清除全部設定資料並回復到出廠的設定。 |
| **索引編號** | 按下方的號碼進入排程設定頁面。 |
| **狀態** | 顯示排程設定是啓動還是關閉。 |

您最多可以設定 15 個排程，然後可以應用於**網際網路連線控制**或是 **VPN** 的**遠端存取控制 LAN-to-LAN** 設定上。

欲新增一個排程，請按任何一個索引號碼，這裡舉索引編號 1 為例。其呼叫排程的細部設定顯示如下：

Applications >> Schedule

Index No. 1

☑ Enable Schedule Setup

| | |
|---|---|
| Start Date (yyyy-mm-dd) | 2000 - 1 - 1 |
| Start Time (hh:mm) | 0 : 0 |
| Duration Time (hh:mm) | 0 : 0 |
| Action | Force On |
| Idle Timeout | 0 minute(s).(max. 255, 0 for default) |

How Often

○ Once

⦿ Weekdays

☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat

OK Clear Cancel

| | |
|---|---|
| **啟用排程設定** | 勾選此項目以啟動此排程。 |
| **開始日期 (yyyy-mm-dd)** | 指定排程的開始日期。 |
| **開始時間 (hh:mm)** | 指定排程的開始時間。 |
| **持續時間 (hh:mm)** | 指定排程的持續時間。 |
| **動作** | 指定呼叫排程能採用的方式：<br>**強迫啟用** - 強迫連線永遠存在。<br>**強迫停用** - 強迫連線永遠停止。<br>**啟用隨選撥接** - 指定隨選播接連線以及閒置的時間。<br>**停用隨選撥接** - 一旦超過閒置時間都沒有任何資料傳輸動作發生，該連線將會停止且在時間排程內都不會再啟用。 |
| **閒置逾時** | 若超過指定時間而沒有任何傳輸動作，系統將中斷連線。 |
| **頻率** | **一次** - 此計劃的頻率只會應用一次。<br>**週期** - 指定一週當中哪些日子需要執行此項排程作業。 |

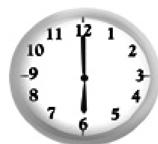
**範例**

假設您想要控制 PPPoE 網際網路存取連線能夠在每天的 9:00 到 18:00 都能保持開啟狀態(強迫啟用)，其他時間則中斷連線(強迫停用)。

**Office Hour:**

**(Force On)**





**Mon - Sun 9:00 am to 6:00 pm**

1. 確定 PPPoE 連線和**時間設定**都能正常運作。
2. 設定 PPPoE 每天早上 9:00 到下午 18:00 都保持連線狀態。
3. 設定每天晚上 18:00 到第二天早上 9:00 都是強迫停用狀態。
4. 在PPPoE網際網路存取設定檔中，指定此二個設定檔，現在PPPoE會依照時間排程，

**強迫啓用**與**強迫停用**來計畫其網際網路連線。

### 4.9.3 RADIUS

撥接使用者遠端認證服務(RADIUS)是一種用戶端/伺服器端安全性驗證之通訊協定，支援驗證、授權和說明，通常為網際網路服務供應商所廣泛應用，是用來作為驗證和授權撥接網路使用者最常見的一種方法。

建立一個 RADIUS 用戶特徵設定，可以讓路由器協助遠端撥入用戶、無線工作站以及 RADIUS 伺服器能夠共同執行驗證的動作,它可集中遠端存取驗證工作以達成網路管理。

Applications >> RADIUS

RADIUS Setup

- [x] Enable

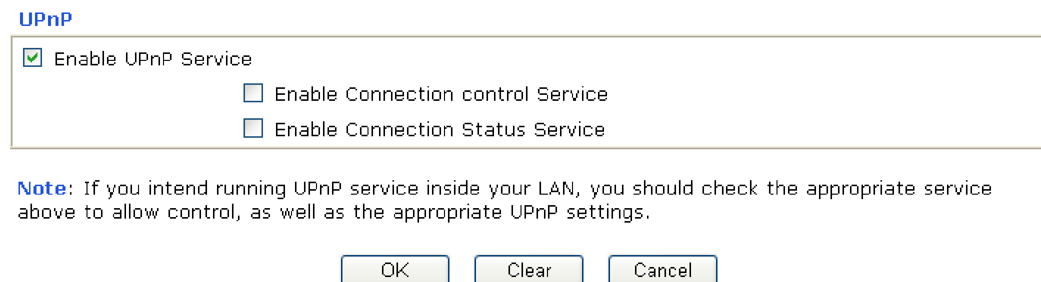
| | |
|---|---|
| Server IP Address | |
| Destination Port | 1812 |
| Shared Secret | |
| Confirm Shared Secret | |

OK  Clear  Cancel

| | |
|---|---|
| **啓用** | 勾選此項以啓動 RADIUS 設定。 |
| **伺服器 IP 位址** | 輸入 RADIUS 伺服器的 IP 位址。 |
| **通訊埠** | 輸入 RADIUS 伺服器所使用的 UDP 通訊埠號，基於 RFC 2138，預設值為 1812。 |
| **共享密碼** | RADIUS 伺服器和用戶共享一個用來驗證二者之間傳遞訊息的密碼，雙方都必須設定相同的共享密碼。 |
| **確認共享密碼** | 請重新輸入共享密碼以確認。 |

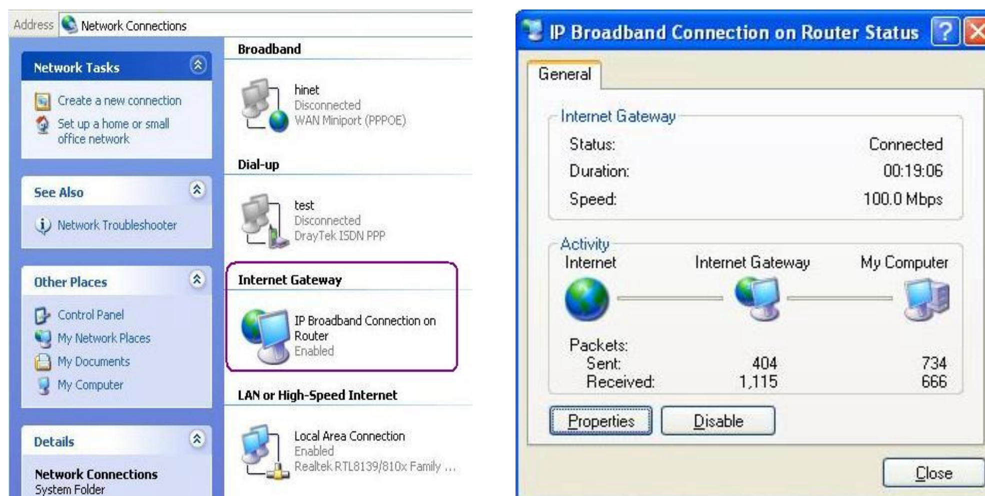
## 4.9.4 UPnP

**UPnP** 協定爲網路連線裝置提供一個簡易安裝和設定介面，爲 Windows 隨插即用系統上的電腦週邊設備提供一個直接連線的方式。使用者不需要手動設定**通訊埠對應**或是 **DMZ**，**UPnP** 只在 Windows XP 系統下可以運作，路由器提供相關的支援服務給 MSN Messenger，允許完整使用聲音、影像和訊息特徵。

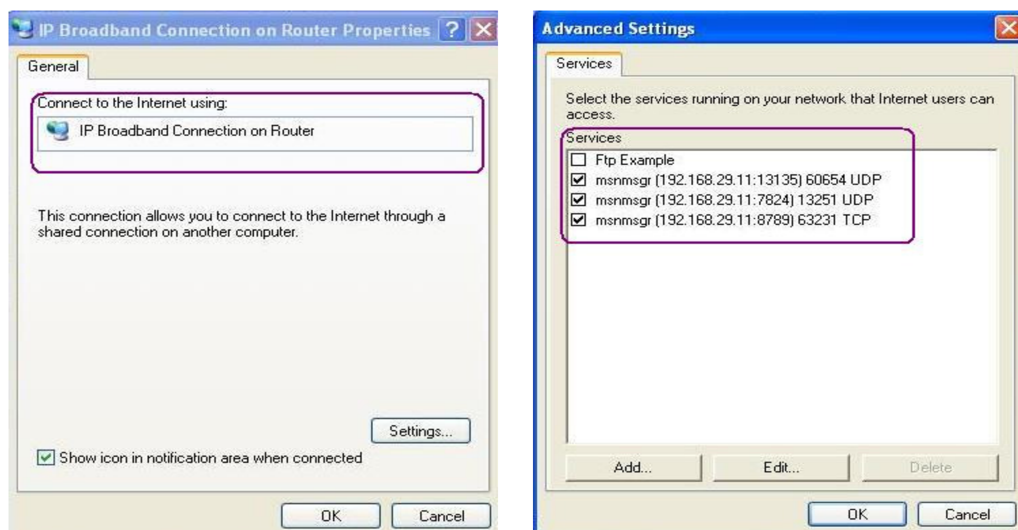



**啓用 UPnP 服務** 您可以視情況勾選**啓用連線控制服務**或是**啓用連線狀態服務**。

在設定**啓用 UPNP 服務**後，在 Windows XP/網路連線上會出現一個 **IP Broadband Connection on Router** 圖示，連線狀態和控制狀態將可開啓使用，NAT Traversal of UPnP 可啓動應用程式中的多媒體特徵，必須手動設定通訊埠對應或是使用其他類似的方法來設定，以下顯示此項功能的範例圖形。




在路由器上的 UPnP 功能，允許應用程式(像是 MSN Messenger, 可察覺出 UPnP 功能) 找到隱藏在 NAT 路由器之下的是什麼，此應用程式也會記住外部 IP 位址並且在路由器上設定通訊埠對應，結果這種能力可將封包自路由器的外部通訊埠傳送到應用程式所使用的內部通訊埠。




有關防火牆與 UPnP 功能之提示–

**無法與防火牆軟體配合**

在您的電腦上啓用防火牆有可能造成 UPnP 不正常運作，這是因爲這些應用程式會擋掉某些網路通訊埠的存取能力。

**安全考量**

在您的網路上啓用 UPnP 功能可能會招致安全威脅，在您啓用 UPnP 功能之前您應該要小心考慮這些風險。

- 某些微軟操作系統已發現到 UPnP 的缺點，因此您需要確定已經應用最新的服務封包。
- 未享有特權的使用者可以控制某些路由器的功能，像是移除和新增通訊埠對應等。

UPnP 功能可不斷變化的新增通訊埠對應來表示一些察覺 UPnP 的應用程式，當這些應用程式不正常的運作中止時，這些對應可能無法移除。

### 4.9.6 網路喚醒(WOL)

區域網路上的電腦可以透過所連結的路由器來喚醒，當使用者想要從路由器喚醒指定的電腦時，使用者必須在此頁面上輸入該電腦正確的 MAC 位址。

此外，此台電腦必須安裝有支援 WOL 功能的網卡，並在 BIOS 設定中開啓 WOL 功能。

Application >> Wake on LAN

Wake on LAN

Note: Wake on LAN integrates with Bind IP to MAC function, only binded PCs can wake up through IP.

Wake by: MAC Address

IP Address: ---

MAC Address: : : : : : Wake Up!

Result

```
 Valid subcommands are:admin          cfg           cmdlog
ftpd          domainname    iface         name
passwd        reboot        autoreboot    commit
```

**喚醒方式** 有二種方式提供給使用者喚醒綁定 IP 的電腦，如果您選擇由 MAC 位址來喚醒的話，您必須輸入該主機正確的 MAC 位址；如果您選擇的是由 IP 位址來喚醒的話，您必須選擇正確的 IP 位址。

喚醒方式: MAC 位址

MAC 位址

IP 位址

**IP 位址** 已在防火牆>>綁定 IP 至 MAC 中設定完成的 IP 位址，將會出現在下拉式清單中，請自清單中選取您想要喚醒的電腦 IP。

**MAC 位址** 輸入被綁定之電腦的 MAC 位址。

**網路喚醒** 按此鈕可以喚醒選定的電腦，喚醒結果將會顯示在方框內。

Application >> Wake on LAN

Wake on LAN

Note: Wake on LAN integrates with Bind IP to MAC function, only binded PCs can wake up through IP.

Wake by: MAC Address

IP Address: ---

MAC Address: : : : : : Wake Up!

Result

```
Send command to client done.
```

# 4.10 VPN 與遠端存取

VPN 是 Virtual Private Network (虛擬私有網路) 的縮寫，是一種利用公眾網路建立一個虛擬的、安全的、方便的通道。企業可透過這個安全通道讓兩個不同地方的辦公室互通內部資料或讓出差在外的辦公人員可以遠端撥入 VPN 通道擷取公司內部的資料。

下圖為 VPN 與遠端存取的主要功能項目：




## 4.10.1 遠端存取控制

這個設定可以啓動必要的 VPN 服務，如果您想要在區域網路中執行 VPN 伺服器功能，您一定要適度關閉路由器的 VPN 服務，讓 VPN 通道暢通，並關閉類似 DMZ 或是開放埠等 NAT 設定。

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

- ☑ Enable PPTP VPN Service
- ☑ Enable IPSec VPN Service
- ☑ Enable L2TP VPN Service

Note: If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

OK　Clear　Cancel

| | |
|---|---|
| **啓用 PPTP VPN 服務** | 勾選此方塊啓動經由 PPTP 通訊協定之 VPN 服務。 |
| **啓用 IPSec VPN 服務** | 勾選此方塊啓動經由 IPSec 通訊協定之 VPN 服務。 |
| **啓用 L2TP VPN 服務** | 勾選此方塊啓動經由 L2TP 通訊協定之 VPN 服務。 |

## 4.10.2 PPP 基本設定

這項功能可以應用在 PPP 相關的 VPN 連線中，諸如 PPTP、L2TP、L2TP over IPSec 等。

VPN and Remote Access >> PPP General Setup

PPP General Setup

| PPP/MP Protocol | | IP Address Assignment for Dial-In Users (When DHCP Disable set) | |
|---|---|---|---|
| Dial-In PPP Authentication | PAP or CHAP | Start IP Address | 192.168.1.200 |
| Dial-In PPP Encryption (MPPE) | Optional MPPE | | |
| Mutual Authentication (PAP) | ○ Yes ⊙ No | | |
| Username | | | |
| Password | | | |

OK

**撥入 PPP 驗證**　選擇此項目強迫路由器以 PAP 協定來驗證撥入使用者。

**PAP 或 CHAP**　選擇此項目表示路由器會嘗試先以 CHAP 協定驗證撥入使用者，如果撥入使用者沒有支援此項協定，系統會改用 PAP 協定來驗證使用者。

**撥入 PPP 加密( MPPE)**　此選項代表 MPPE 加密方式是由路由器針對遠端撥入使用者選擇性採用的方法，如果遠端撥入使用者沒有支援 MPPE 加密演算式，路由器將會傳送無 MPPE 加密封包出去，否則 MPPE 加密將直接用於資料加密處理。

Optional MPPE
Optional MPPE
Require MPPE(40/128 bit)
Maximum MPPE(128 bit)

**MPPE (40/128bit) -** 選擇此項目可以強迫路由器利用 MPPE 加密演算式加密資料封包，此外遠端撥入使用者在使用 128-bit 之前可先使用 40-bit 執行加密動作，換言之，如果沒有支援 128-bit 加密法，系統將會自動使用 40-bit 加密方式於資料加密上。

**MPPE (128bit) -**此選項指出路由器將會使用 MPPE 最大值(128 bits)來加密資料。

**雙方共同驗證 (PAP)**　共同驗證功能主要應用於和其他路由器或是需要雙向驗證的用戶連絡，以便取得更佳安全性能，因此當您的對點路由器需要共同驗證時，您就應該啟動此功能，並進一步指定使用者名稱和密碼。

**起始 IP 位址**　輸入撥入 PPP 連線的 IP 位址，您應該自本地虛擬網路中選擇一個 IP 位址，例如假設本地虛擬網路為 192.168.1.0/255.255.255.0，您可以選擇 192.168.1.200 做為起始 IP 位址，但您必須注意到前二個 IP 位址 192.168.1.200 和 192.168.1.201 乃是保留作為 ISDN 遠端撥入使用者所使用。

### 4.10.3 IPSec 基本設定

在 **IPSec 基本設定**中，有二種主要的配置方式。

- 第一階段：IKE 參數的協商作業包含加密、重述、Diffie-Hellman 參數值和壽命，以保護後續 IKE 交換、使用預先共同金鑰或是數位簽章(x.509)之對等驗證。協商程序

起始方提出所有的原則給遠端的另一方，遠端一方嘗試尋找符合其政策之最高優先權，最後建立一個 IKE 階段 2 的安全通道。

- 第二階段：IPSec 安全協商包含驗證封包頭(AH)或是 ESP，供後續 IKE 交換和雙邊安全通道設立之檢測之用。

在 IPSec 中有二種加密方式 – 傳送與通道，傳送模式將會增加 AH/ESP 承載量並使用原始 IP 標頭來加密承載的資料，此模式只應用於本地封包上如 L2TP over IPSec，通道模式不只增加 AH/ESP 承載量也會使用新的 IP 封包頭來加密整個原始 IP 封包。

驗證封包頭(AH) 提供 VPN 雙方的 IP 封包資料驗證和整合，可以單方重述功能來達成建立訊息摘要的動作，這些摘要隨著封包傳送將放置於封包頭。接收方將會在封包上執行同樣的動作，並與所接收到的數值比較。

封裝式安全酬載(ESP)提供選擇性驗證方法，對資料機密化和防護的安全協定，可重新進行檢測。

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Pre-Shared Key

Confirm Pre-Shared Key

IPSec Security Method

☑ Medium (AH)

Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

OK Cancel

**IKE 認證方式**

通常應用在遠端撥入使用者或是使用動態 IP 位址的節點(LAN-to-LAN)以及 IPSec 相關之 VPN 連線上，像是 L2TP over IPSec 和 IPSec 通道。

**預先共用金鑰** - 只有支援預先共用金鑰，請指定一個金鑰作爲 IKE 驗證之用。

**確認預先共用金鑰**- 確認您所輸入的共用金鑰。

**IPSec 安全防護方式**

**中級 (AH)** - 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。

**高級 (ESP)** - 表示資料將被加密及驗證，請自下 DES、3DES 或 AES 中選取適合項目。

## 4.10.4 IPSec 端點辨識

路由器提供 32 種 IPSec 端點辨識設定檔：

VPN and Remote Access >> IPSec Peer Identity

X509 Peer ID Accounts: | Set to Factory Default |

| Index | Name | Status | Index | Name | Status |
|---|---|---|---|---|---|
| 1. | ??? | X | 17. | ??? | X |
| 2. | ??? | X | 18. | ??? | X |
| 3. | ??? | X | 19. | ??? | X |
| 4. | ??? | X | 20. | ??? | X |
| 5. | ??? | X | 21. | ??? | X |
| 6. | ??? | X | 22. | ??? | X |
| 7. | ??? | X | 23. | ??? | X |
| 8. | ??? | X | 24. | ??? | X |
| 9. | ??? | X | 25. | ??? | X |
| 10. | ??? | X | 26. | ??? | X |
| 11. | ??? | X | 27. | ??? | X |
| 12. | ??? | X | 28. | ??? | X |
| 13. | ??? | X | 29. | ??? | X |
| 14. | ??? | X | 30. | ??? | X |
| 15. | ??? | X | 31. | ??? | X |
| 16. | ??? | X | 32. | ??? | X |

| | |
|---|---|
| **回復出廠預設值** | 按此鈕清除全部設定。 |
| **索引** | 請按索引下方的號碼以進入設定頁面。 |
| **名稱** | 顯示 LAN-to-LAN 設定檔案中特定撥入使用者的使用者名稱，符號**???**代表該設定檔是空的，未做任何設定。 |

點選每個索引號碼以便編輯遠端使用者設定檔，每個撥入類型需要您在右邊填入不同資訊，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。

VPN and Remote Access >> IPSec Peer Identity

Profile Index : 1

Profile Name ???

☑ Enable this account

◉ Accept Any Peer ID

○ Accept Subject Alternative Name

Type IP Address

IP

○ Accept Subject Name

Country (C)

State (ST)

Location (L)

Orginization (O)

Orginization Unit (OU)

Common Name (CN)

Email (E)

OK Clear Cancel

**設定檔名稱** 請輸入此設定檔的檔名。

**接收任何對方 ID** 按此鈕可以接受任何一個電腦的連線而不理會它是誰。

**接受主體替代名稱** 按此鈕以決定特定之數位簽章接受符合要求的對手，本區可以是 IP 位址、網域或是電子郵件，類型下方區域方塊依據您所選的類型而有所不同，請按照實際需要填入必要資訊。

**接受主體名稱** 按此鈕讓特定區域的數位簽章能接受符合要求的對手，本區包含有國家、狀態、居住地區、組織、單位、常用名稱及電子郵件等等。

### 4.10.5 遠端撥入使用者

藉由維護遠端使用者設定檔表格，您可以管理遠端存取狀況，這樣使用者可以經由驗證得以撥入或是建立 VPN 連線。您可以設定包含指定連線對點 ID、連線 ID (PPTP、IPSec Tunnel 以及 L2TP 和 L2TP over IPSec)等參數，和相關安全防護方式。

路由器提供 32 種存取使用者號碼予撥入用戶，此外經由內建 RADIUS 用戶端功能，您可以將帳號延伸至 RADIUS 伺服器。下圖顯示帳號總表格：

VPN and Remote Access >> Remote Dial-in User

Remote Access User Accounts: | Set to Factory Default |

| Index | User | Status | Index | User | Status |
|---|---|---|---|---|---|
| 1. | ??? | X | 17. | ??? | X |
| 2. | ??? | X | 18. | ??? | X |
| 3. | ??? | X | 19. | ??? | X |
| 4. | ??? | X | 20. | ??? | X |
| 5. | ??? | X | 21. | ??? | X |
| 6. | ??? | X | 22. | ??? | X |
| 7. | ??? | X | 23. | ??? | X |
| 8. | ??? | X | 24. | ??? | X |
| 9. | ??? | X | 25. | ??? | X |
| 10. | ??? | X | 26. | ??? | X |
| 11. | ??? | X | 27. | ??? | X |
| 12. | ??? | X | 28. | ??? | X |
| 13. | ??? | X | 29. | ??? | X |
| 14. | ??? | X | 30. | ??? | X |
| 15. | ??? | X | 31. | ??? | X |
| 16. | ??? | X | 32. | ??? | X |

| | |
|---|---|
| **回復出廠預設值** | 按此鈕清除全部設定。 |
| **索引** | 請按索引下方的號碼以進入遠端撥入使用者之設定頁面。 |
| **用戶** | 顯示 LAN-to-LAN 設定檔案中特定撥入使用者的使用者名稱，符號**???**代表該設定檔是空的，未做任何設定。 |
| **狀態** | 顯示特定撥入使用者的存取狀態，符號 V 和 X 分別代表活動中與不活動的檔案。 |

點選每個索引號碼以便編輯遠端使用者設定檔，每個撥入類型需要您在右邊填入不同資訊，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。

VPN and Remote Access >> Remote Dial-in User

Index No. 1

**User account and Authentication**

- [ ] Enable this account
- Idle Timeout 300 second(s)

**Allowed Dial-In Type**

- [x] PPTP
- [x] IPSec Tunnel
- [x] L2TP with IPSec Policy None

- [ ] Specify Remote Node
- Remote Client IP or Peer ISDN Number
- or Peer ID
- Netbios Naming Packet ● Pass ○ Block

Username ???

Password

**IKE Authentication Method**

- [x] Pre-Shared Key
- IKE Pre-Shared Key
- [ ] Digital Signature(X.509)
- None

**IPSec Security Method**

- [x] Medium(AH)
- High(ESP) [x] DES [x] 3DES [x] AES
- Local ID (optional)

OK Clear Cancel

| | |
|---|---|
| **開啓這個帳號** | 勾選此方塊以啓用此功能。<br>**閒置逾時 -** 如果撥入使用者閒置超過所設定的時間，路由器將會自動中斷連線，預設閒置逾時爲 300 秒。 |
| **PPTP** | 爲伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。 |
| **IPSec 通道** | 允許遠端撥入使用者透過網際網路觸發 IPSec VPN 連線。 |
| **具有 IPSec 原則的 L2TP** | 爲伺服器建立一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取：<br>**無 -** 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。<br>**建議選填 -**如果在整個連線過程中完全可以運用，此選項會先應用 IPSec 原則。否則撥入 VPN 連線會成爲一種完全的 L2TP 連線。<br>**必須 -** 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。 |
| **指定遠端節點** | **勾選 -** 您可以指定遠端撥入使用者或是對點 ID (應用於 IKE 主動模式中)的 IP 位址。<br>**不勾選 -** 表示您所選擇的連線類型，將會應用**一般設定**中所設定的驗證方式和安全防護方式。 |
| **使用者名稱** | 當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 |
| **密碼** | 當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 |
| **IKE 驗證方式** | **預先共同金鑰-** 勾選此方塊啓用此功能並輸入 1-63 文字做爲預先共同金鑰。<br>**數位簽章 (X.509) –**勾選此方塊啓用此功能並選擇一組事先定義的簽章內容 (在 **VPN 和遠端存取>>IPSec 端點辨識**中設定)。 |
| **安全防護方式** | 對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區爲必要設定。請勾選中級或是高級設定作爲安全防護方式。<br>**中級 -Authentication Header (AH)**表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。<br>**高級 -Encapsulating Security Payload (ESP)**表示資料將被加密及驗證，請自下拉式清單中選取適合項目。<br>**本機 ID -**指定一個本地 ID 以便作爲 LAN-to-LAN 的撥入設定，此項是選擇項目且只能應用在 IKE 主動模式上。 |

### 4.10.6 設定 LAN to LAN

您可以透過維護連線檔案的表格來管理 LAN-to-LAN 連線，您可設定包含指定連線方向(撥進或是撥出)的參數、連線對方的 ID、連線型態(VPN 含 PPTP, IPSec Tunnel 和 L2TP 或是其他)以及相關的安全防護方法等等。

路由器提供 32 個設定檔，也就是說同時可以支援 2 個 VPN 頻道，下圖顯示設定檔案的清單表格。

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: | Set to Factory Default |

| Index | Name | Status | Index | Name | Status |
|---|---|---|---|---|---|
| 1. | ??? | X | 17. | ??? | X |
| 2. | ??? | X | 18. | ??? | X |
| 3. | ??? | X | 19. | ??? | X |
| 4. | ??? | X | 20. | ??? | X |
| 5. | ??? | X | 21. | ??? | X |
| 6. | ??? | X | 22. | ??? | X |
| 7. | ??? | X | 23. | ??? | X |
| 8. | ??? | X | 24. | ??? | X |
| 9. | ??? | X | 25. | ??? | X |
| 10. | ??? | X | 26. | ??? | X |
| 11. | ??? | X | 27. | ??? | X |
| 12. | ??? | X | 28. | ??? | X |
| 13. | ??? | X | 29. | ??? | X |
| 14. | ??? | X | 30. | ??? | X |
| 15. | ??? | X | 31. | ??? | X |
| 16. | ??? | X | 32. | ??? | X |

| | |
|---|---|
| **回復出廠預設值** | 按此鈕清除全部設定。 |
| **名稱** | 意即 LAN-to-LAN 檔案名稱，**???**符號代表該檔案目前是空的。 |
| **狀態** | 表示個別檔案的狀態，符號 V 和 X 分別代表使用中與未使用的檔案。 |

請按索引編號連結以編輯個別設定檔，按下後可看到如下的頁面，每個 LAN-to-LAN 檔案包含有四個子群組，如果該區域是灰色的，即表示您無法在該項目做任何設定，下面的說明可以引導您於各個設定區填入相關資訊。

由於網頁太長，我們將之切成數個段落來說明。

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name ???

Enable this profile

Netbios Naming Packet ◉Pass ○Block

Call Direction ◉ Both ○ Dial-Out ○ Dial-In

Always on

Idle Timeout 300 second(s)

Enable PING to keep alive

PING to the IP

2. Dial-Out Settings

Type of Server I am calling

○ PPTP

○ IPSec Tunnel

○ L2TP with IPSec Policy None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

Username ???

Password

PPP Authentication PAP/CHAP

VJ Compression ◉ On ○ Off

IKE Authentication Method

◉ Pre-Shared Key

IKE Pre-Shared Key

○ Digital Signature(X.509)

None

IPSec Security Method

◉ Medium(AH)

○ High(ESP) DES without Authentication

Advanced

Index(1-15) in Schedule Setup:

, , ,

**設定檔名稱** 針對此 LAN-to-LAN 連線，請指定一個設定檔案名稱。

**啓用此設定檔** 按此方塊啓用此設定檔。

**撥號方向** 針對此 LAN-to-LAN 連線，請指定允許的撥號方向。
**雙向** – 發話方/接話方
**撥出** - 發話方
**撥入** - 接話方

**永遠連線或閒置逾時** **永遠連線** – 勾選此方塊讓路由器永遠保持 VPN 連線。
**閒置逾時** - 預設值爲 300 秒，若連線閒置時間超過此數值，路由器將自動中斷連線。

**啓用 PING 以維持連線** 此功能可協助路由器決定 IPSec VPN 連線狀態，對不正常的 IPSec VPN 通道中斷尤其有用。詳細內容請參考下面的註解，請勾選此方塊啓動 PING 封包傳輸至指定的 IP 位址。

**指定 IP 位址** 輸入位於 VPN 通道另一邊的遠端主機的虛擬 IP 位址。

> **註解：啓用 PING 以維持連線**用來管理不正常的 IPSec VPN 連線中斷，提供一個 VPN 連線狀態供路由器判斷是否需要重撥。
> 正常而言，如果 VPN 任何一方想要中斷連線，那麼就必須依照封包交換程序通知對方。不過如果另一方在未通

知的情況下中斷連線，Vigor 路由器將無從得知此項訊息，為了解決這樣的困境，藉著不斷傳送 PING 封包至遠端主機的方式，路由器就可以知道此項 VPN 通道有無實際運作，這是一種獨立的 DPD (無效對方檢測)。

**PPTP**

為伺服器建立一個透過網際網路的 PPTP VPN 連線，您必須設定連線類型和身分辨識像是使用者名稱與密碼等，以便驗證遠端伺服器。

**IPSec 通道**

為伺服器建立一個透過網際網路的 IPSec VPN 連線。

**具有 IPSec 原則的 L2TP**

為伺服器建立一個透過網際網路的 L2TP VPN 連線。您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取：

**無 -** 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP，可以在完全 L2TP 連線中檢視內容。

**建議選填 -**如果在整個連線過程中是可以運用的情形下，此選項會先應用 IPSec 原則。否則撥出 VPN 連線會成為一種完全的 L2TP 連線。

**一定要有 -** 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。

**使用者名稱**

當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。

**密碼**

當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。

**PPP 認證**

當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。PAP/CHAP 是最平常的選項。

**VJ 壓縮**

當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。VJ 壓縮可作為 TCP/IP 協定標頭壓縮之用，通常設定選擇**開啓**以改善頻寬利用的狀況。

**IKE 驗證方式**

**預先共用金鑰-** 勾選此方塊啓用此功能並按 **IKE 預先共用金鑰**按鈕輸入金鑰及確認金鑰。

**數位簽章 (X.509) –**勾選此方塊啓用此功能並選擇一組事先定義的簽章內容 (在 **VPN 和遠端存取>>IPSec 端點辨識**中設定)。

**IPSec 安全防護方式**

對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區為必要設定。

**中級 (AH)** 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。

**高級 (ESP-Encapsulating Security Payload)** 表示資料將被加密及驗證，請自下拉式清單中選取適合項目：

***DES 無驗證*** - 使用 DES 加密演算式，但不採用任何驗證計畫。

***DES 有驗證* -** 使用 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。

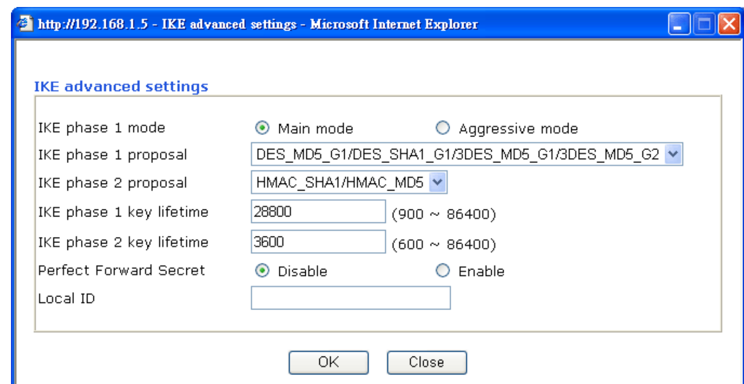
***3DES 無驗證*** - 使用三重 DES 加密演算式，但不採用任何驗證計畫。

***3DES 有驗證*** **-**使用三重 DES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。

***AES 無驗證*** - 使用 AES 加密演算式，但不採用任何驗證計畫。

***AES 有驗證*** **-**使用 AES 加密演算式，且採用 MD5 或 SHA-1 驗證計畫。

**進階** 指定模式、建議和 IKE 階段金鑰有效時間等設定，可按**進階**按鈕進入進階設定，視窗顯示如下：




**IKE 階段 1 模式 –** 選擇 **Main 模式**或是 **Aggressive 模式**。比起 **Aggressive 模式**，**Main 模式**顯得更加安全，因為在安全通道中有更多的交換動作於此完成，不過，**Aggressive 模式**是比較快速的模式。路由器的預設值為 **Main 模式**。

**IKE 階段1 建議 -** 針對 VPN 通道另一方可提供本地有效的驗證計畫及加密演算式，並取得回覆訊息以找出符合的結果。對 **Aggressive 模式**來說有二種有效的組合方式，對 **Main 模式**來說有九種有效的組合方式，建議您選擇能涵蓋多數計畫的組合方式。

**IKE 階段2 建議 -** 針對 VPN 通道另一方可提供本地有效的驗證計畫及加密演算式，並取得回覆訊息以找出符合的結果。對 **Aggressive 模式**來說有二種有效的組合方式，對二種模式來說有 3 種有效的組合方式，建議您選擇能涵蓋多數計畫的組合方式。

**IKE 階段 1 金鑰有效時間-** 考慮到安全之故，使用者必須訂定有效時間，預設值為 28800 秒，您可以在 900 與 86400 秒之間指定所需的時間值。

**IKE 階段 2 金鑰有效時間-** 考慮到安全之故，使用者必須訂定有效時間，預設值為 3600 秒，您可以在 900 與 86400 秒之間指定所需的時間值。

**本機 ID –** 在 **Aggressive 模式**中，當鑑定遠端 VPN 伺服器身分時，本機 ID 代表 IP 位址，ID 長度限制於 47 個字元。

3. Dial-In Settings

Allowed Dial-In Type

☑ PPTP
☑ IPSec Tunnel
☑ L2TP with IPSec Policy [None]

☐ Specify Remote VPN Gateway
Peer VPN Server IP
or Peer ID

Username [???]
Password
VJ Compression ◉ On ○ Off

IKE Authentication Method
☑ Pre-Shared Key
IKE Pre-Shared Key
☐ Digital Signature(X.509)
None

IPSec Security Method
☑ Medium(AH)
High(ESP) ☑ DES ☑ 3DES ☑ AES

4. TCP/IP Network Settings

| | |
|---|---|
| My WAN IP | 0.0.0.0 |
| Remote Gateway IP | 0.0.0.0 |
| Remote Network IP | 0.0.0.0 |
| Remote Network Mask | 255.255.255.0 |

More

RIP Direction [Disable]
From first subnet to remote network, you have to do [Route]

☐ Change default route to this VPN tunnel ( Only single WAN supports this )

OK Clear Cancel

| | |
|---|---|
| **允許的撥入類型** | 以不同類型來決定撥入連線。 |
| **PPTP** | 允許遠端撥入用戶透過網際網路達成 PPTP VPN 連線，請設定遠端撥入用戶的使用者名稱和密碼。 |
| **IPSec 通道** | 允許遠端撥入用戶透過網際網觸發 IPSec VPN 連線。 |
| **具有 IPSec 原則的 L2TP** | 允許遠端撥入用戶透過網際網路製造 L2TP VPN 連線，您可以選擇使用單獨 L2TP 或是含有 IPSec 的 L2TP，請自下拉式選項選取：<br>**無 -** 此選項完全不會應用 IPSec 原則，VPN 連線採用不帶有 IPSec 原則的 L2TP 可以在完全 L2TP 連線中檢視內容。<br>**建議選填-**如果在整個連線過程中是可以運用的情形下，此選項會先應用 IPSec 原則。否則撥出 VPN 連線會成為一種完全的 L2TP 連線。<br>**必須 -** 此選項可在 L2TP 連線中明確指定所要運用的 IPSec 原則。 |
| **指定 ISDN CLID 或 遠端 VPN 閘道** | 您可勾選此項，並指定遠端撥入用戶的真實 IP 位址或 ID (必須與撥入類型中所設定的 ID 相同)。<br>若您選擇 ISDN 類型，請於此輸入對方的 ISDN 號碼，(適用於 *i* 機型 )。<br><br>此外針對 VPN 功能，您應該進一步指定右邊相關安全設定。 |
| **使用者名稱** | 當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 |

| | |
|---|---|
| **密碼** | 當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。 |
| **VJ 壓縮** | 當您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時，本區是可應用的。VJ 壓縮可作為 TCP/IP 協定標頭壓縮之用。 |
| **IKE 驗證方式** | 當您指定遠端節點的 IP 位址時，IKE 驗證可套用在 IPSec 通道和含 IPSec 原則之 L2TP 上。不過，不管有沒有指定遠端節點的 IP 位址予 IPSec 通道使用，您仍然可以設定數位簽章(X.509)。<br>**預先共同金鑰-** 勾選此方塊啓用此功能並按 **IKE 預先共用金鑰**按鈕輸入金鑰及確認金鑰。<br>**數位簽章 (X.509) –**勾選此方塊啓用此功能並自下拉式清單中選擇 **VPN 遠端存取控制>>IPSec 端點辨識**中所預先定義的設定檔。 |
| **IPSec 安全防護方式** | 當您指定遠端模式時，對 IPSec 通道和 L2TP 含 IPSec 原則來說，本區為必要設定。<br>**中級 (AH)** 表示資料將被驗證，但未被加密，此選項的預設時是勾選狀態。<br>**高級 (ESP-Encapsulating Security Payload)-** 表示資料將被加密及驗證，請自下拉式清單中選取適合項目。 |
| **我的 WAN IP** | 本區只在您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時有效。預設值為 0.0.0.0，表示 Vigor 路由器在 IPCP 協商階段期間，將從遠端路由器取得您所指定的 IP 位址，請在此輸入 IP 位址。此一位址適用於本機為 VPN client (dial-out) 端時。 |
| **遠端閘道 IP** | 本區只在您選擇 PPTP 或是 L2TP 含/不含 IPSec 原則時有效。預設值為 0.0.0.0，表示 Vigor 路由器在 IPCP 協商階段期間，將發予對方的 IP 位址，請在此輸入發予對方之 IP 位址。此一位址適用於本機為 VPN Server (dial-in) 端時。 |
| **遠端網路 IP/遠端網路遮罩** | 新增一個靜態路由以便透過網際網路，引導遠端網路 IP 位址/遠端網路遮罩預定之全部傳輸流量。對 IPSec 而言，這項設定是第二階段快速模式的目的用戶端之身分。 |
| **更多** | 新增一個靜態路由，並藉由網際網路引導更多的遠端網路 IP 位址/遠端網路遮罩預定之全部傳輸流量。通常在您發現遠端 VPN 路由器有數個子網路存在時，您會使用此按鈕設定更多的路由。 |
| **RIP 方向** | 此選項指定 RIP (路由資訊協定) 封包的方向，您可以啓用也可以停用 RIP 方向，於此，我們提供您四種選擇：TX/RX 二者均有、TX、RX 以及停用。 |
| **從第一個子網路到遠端網路，您必須要作** | 如果遠端網路只允許您以單一 IP 撥號，請選擇 **NAT** 否則請選擇**路由**。 |
| **變更預設路由此 VPN 通道** | 勾選此方塊變更此 VPN 通道的預設路由，注意此設定只有在一個 WAN 介面啓用時有效，若是二個 WAN 介面皆啓用，此功能即無法使用。 |

### 4.10.7 連線管理

您可以查看全部 VPN 連線的總結清單，您可中斷任何一個 VPN 連線，只要輕輕按下中斷按鈕即可。您也可以使用撥出工具並按**撥號**按鈕主動撥出任何的電話。

VPN and Remote Access >> Connection Management

Dial-out Tool　　Refresh Seconds : 10　Refresh

Dial

VPN Connection Status

Current Page: 1　　Page No.　Go　>>

| VPN | Type | Remote IP | Virtual Network | Tx Pkts | Tx Rate (Bps) | Rx Pkts | Rx Rate (Bps) | UpTime |
|---|---|---|---|---|---|---|---|---|

xxxxxxxx : Data is encrypted.
xxxxxxxx : Data isn't encrypted.

| | |
|---|---|
| **撥號** | 按此鈕執行撥號功能。 |
| **更新間隔秒數** | 選擇重新顯示狀態的間隔秒數，有 5、10、30 秒等三種選擇。 |
| **更新頁面** | 按此鈕以重新顯示整個連線狀態。 |

# 4.11 憑證管理

數位憑證就像是一個電子 ID，此 ID 可以由憑證授權中心註冊取得。它包含有您的名字、序號、到期日、憑證授權的數位簽章，這樣一來，接收者可以確認該憑證是否是真實的。本路由器支援遵守標準 X.509 的數位憑證。

任何想要使用數位憑證的人都應該先有 CA 伺服器註冊的憑證，此憑證也可從其他具公信力的 CA 伺服器取得，如此還可以驗證其他從公信力的 CA 伺服器取得憑證的另一方。

此處您可以管理產生本機的數位憑證，並設定具公信力之 CA 憑證，使用憑證前，請記得調整路由器的時間，這樣才可取得正確的憑證有效期。

下圖顯示憑證管理的功能項目：




## 4.11.1 本機憑證

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

| Name | Subject | Status | Modify |
| --- | --- | --- | --- |
| Local | --- | --- | View Delete |

GENERATE IMPORT REFRESH

X509 Local Certificate

**產生** 按此鈕以開啓**產生憑證需求**視窗。

Certificate Management >> Local Certificate

Generate Certificate Request

Subject Alternative Name

| | |
|---|---|
| Type | IP Address |
| IP | |

Subject Name

| | |
|---|---|
| Country (C) | |
| State (ST) | |
| Location (L) | |
| Orginization (O) | |
| Orginization Unit (OU) | |
| Common Name (CN) | |
| Email (E) | |

| | |
|---|---|
| Key Type | RSA |
| Key Size | 1024 Bit |

Generate

輸入全部的資訊，然後再按一次**產生**按鈕。

**匯入** 按此鈕以匯入儲存的檔案作爲憑證資訊。

**頁面更新** 按此鈕以更新資訊。

**檢視** 按此鈕以檢視憑證詳細的設定。

在按下**產生**按鈕之後，產生後的資訊將會顯示在視窗上，見下圖：

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

| Name | Subject | Status | Modify |
|---|---|---|---|
| Local | /C=TW/ST=HC/L=HC/O=Draytek/O... | Requesting | View Delete |

GENERATE IMPORT REFRESH

X509 Local Certificate


```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH
EwJIQzEQMA4GA1UEChMHRHJheXRlazELMAkGA1UECxMCUkQxIjAgBgkqhkiG9w0B
CQEWE3N1cHBvcnRAZHJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTU5HQvXpAzcrgJBGrikTUBX
a1X//fgnEccQA2LPSQIQ85Qychwq07Bm0EDf10wHwCalAZQoGvIiODMC7f5w9xA8
m6+0f4xZ4QQnjXXgciC0Bj1iAa6MLScelsynZhkgnQ1QN5uFAgMBAAGgADANBgkq
hkiG9w0BAQUFAAOBgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYDZefCmGfX
9yojHpstNsmWsMRuAwGeKCWc8S/gLtHhr6iccMoToQFx/LWdaEPU5LqryBKKgC9t
eorpDa1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==
-----END CERTIFICATE REQUEST-----
```

## 4.11.2 具公信力之 CA 憑證

具公信力之 CA 憑證列出三組具公信力之 CA 憑證表。

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

| Name | Subject | Status | Modify |
|---|---|---|---|
| Trusted CA-1 | --- | --- | View Delete |
| Trusted CA-2 | --- | --- | View Delete |
| Trusted CA-3 | --- | --- | View Delete |

IMPORT REFRESH

若要輸入事先儲存的具公信力之 CA 憑證，請按**匯入**鈕開啓如下的視窗，並使用**瀏覽**…找到儲存的文字檔案，接著按下**匯入**鈕，您所要匯入的檔案將會列在視窗上，再按一次**匯入**鈕即可使用預先儲存的檔案。

Certificate Management >> Trusted CA Certificate

Import X509 Trusted CA Certificate

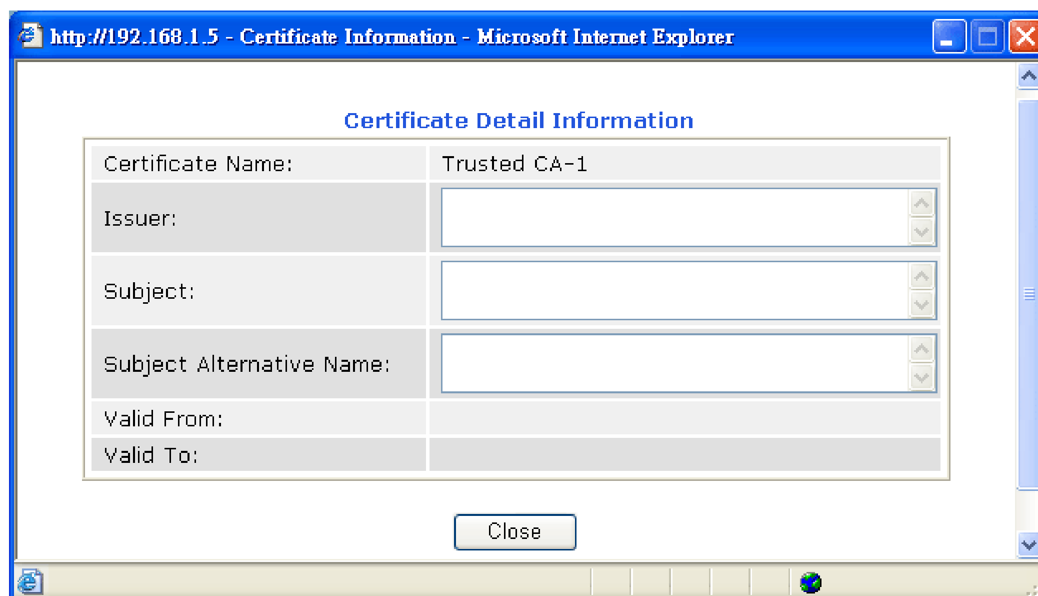
Select a trusted CA certificate file.

Browse...

Click Import to upload the certification.

Import Cancel

如要檢視每個具公信力之 CA 憑證，請按**檢視**按鈕開啓憑證的詳細資訊視窗，如果您想要刪除 CA 憑證，選擇該憑證並按下**刪除**按鈕，所有相關的憑證資訊即可刪除。



### 4.11.3 憑證備份

路由器的本機憑證與具公信力之 CA 憑證可以儲存爲一個檔案，請按下述畫面的備份按鈕來儲存，如果您想要設定加密的密碼，請在加密密碼與確認密碼二欄中輸入所需的字元。

Certificate Management >> Certificate Backup

Certificate Backup / Restoration

Backup

Encrypt password:

Confirm password:

Click Backup to download certificates to your local PC as a file.

Restoration

Select a backup file to restore.

Browse..

Decrypt password:

Click Restore to upload the file.

## 4.12 VoIP

Voice over IP network (VoIP)可讓您使用寬頻網際網路連線撥打網路電話。

有很多種不同的電話信號協定、方法可讓 VoIP 裝置使用以便與對方溝通聯繫，最普遍的協定有 SIP、MGCP、Megaco 和 H.323，這些協定彼此都不完全相容(除非是透過軟體伺服器的掌控)。

Vigor V 系列機種支援 SIP 協定，因爲此種協定對 ITSP (Internet Telephony Service Provider)而言是很理想也很方便，支援也最廣。SIP 是一種端對端信號協定，可建立使用者於 VoIP 結構中之出席情形和機動性。每個想要使用 SIP 相同資源辨識器之用戶都可使用標準的 SIP URI 格式

**sip: user:password @ host: port**

某些區域可能有不同的使用方式，一般來說主機指的是網域，使用者資訊包含有使用者名稱區、密碼區，@符號則緊跟在後，這種格式和 URL 很相似，所以有些人以 SIP URL 來稱呼它。SIP 支援點對點直接撥號，同時也可透過 SIP 代理伺服器(角色雷同 H.323 Gatekeeper)來撥號，而 MGCP 協定則是使用用戶-伺服器結構，撥號方式和目前 PSTN 網路是相同的。

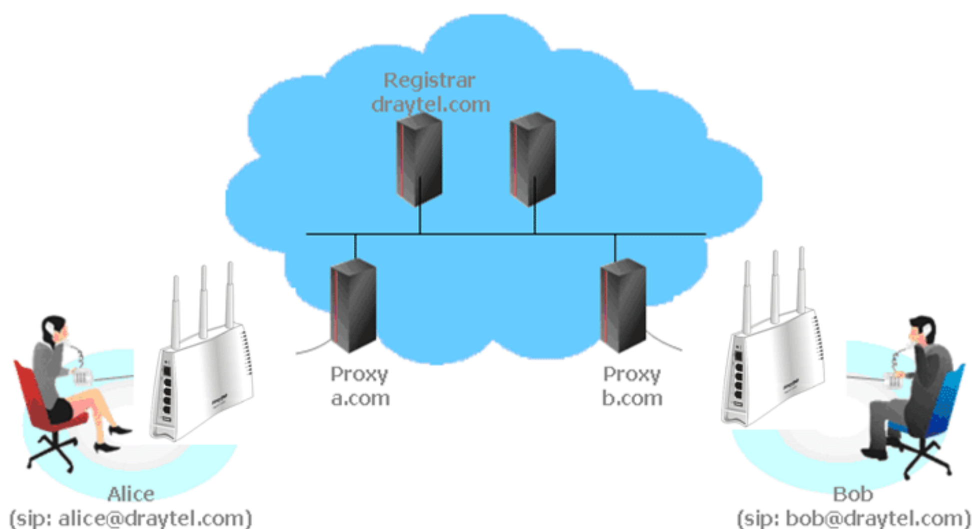
在撥號設定之後，聲音是透過 RTP (Real-Time Transport Protocol)來傳送的，不同的 codecs(用來壓縮和解壓縮聲音)可以包覆於 RTP 封包中，Vigor V 機種提供不同的 codecs 包括 G.711 A/μ-law, G.723, G.726 和 G.729 A & B，每個 codecs 都使用不同頻寬，因此可以提供不同等級的聲音品質。Codec 使用的頻寬越多，聲音品質越好，雖然如此還是應該配合您的網際網路頻寬選擇適宜的 codec 才恰當。

通常有二種撥號類型，說明如下：

- **透過 SIP 伺服器撥號**

  首先 Vigor V 機種必須先向 SIP 註冊，傳送註冊訊息才可生效，然後雙方的 SIP 代理商將轉送一系列訊息給與撥號者，以便建立完整的 session。

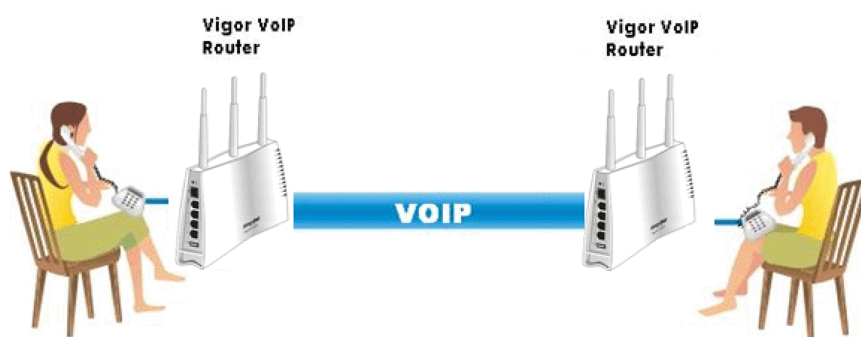
如果雙方都向相同 ISP 業者註冊，那麼我們可以下圖來做簡單說明：




這種模式最主要的好處是您不必去記朋友的 IP 位址(因為它可能常常會改變，如果該位址是浮動的位址的話)，相反的您只要使用撥號計畫或是直接撥朋友的帳號名稱就可以了。

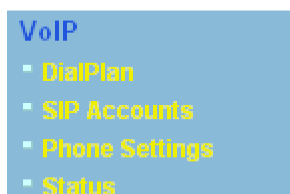
- **點對點**

  在撥打電話之前，您必須知道朋友的 IP 位址，Vigor VoIP 路由器會建立雙方間的連線。




我們的 Vigor V 機種首先採用有效之 codecs，但同時也擔保自動 QoS 的功能，QoS 擔保可以協助指定聲音流量較高之優先權，您對聲音所需求之 inbound 和 outbound 頻寬永遠擁有優先處理權，但是您的資料處理就會有些慢，不過還在忍受範圍內。

下圖為 VoIP 的功能項目：




### 4.12.1 撥號對應表

本頁讓使用者設定 VoIP 功能所需的電話簿及數字對應設定。請按頁面上的連結進入下一層設定頁面。

VoIP >> DialPlan Setup

DialPlan Configuration

| |
|---|
| Phone Book |
| Digit Map |
| Call Barring |
| Regional |
| PSTN Setup |

## 電話簿

在本節中，您可以設定 VOIP 電話，這個設定可以幫助用戶以最快且最簡單的方式撥出電話號碼。本頁總共提供 60 組號碼給用戶儲存朋友以及家人的 SIP 位址。

VoIP >> DialPlan Setup

Phone Book

| Index | Phone number | Display Name | SIP URL | Dial Out Account | Loop through | Backup Phone Number | Status |
|---|---|---|---|---|---|---|---|
| 1. | | | | Default | None | | x |
| 2. | | | | Default | None | | x |
| 3. | | | | Default | None | | x |
| 4. | | | | Default | None | | x |
| 5. | | | | Default | None | | x |
| 6. | | | | Default | None | | x |
| 7. | | | | Default | None | | x |
| 8. | | | | Default | None | | x |
| 9. | | | | Default | None | | x |
| 10. | | | | Default | None | | x |
| 11. | | | | Default | None | | x |
| 12. | | | | Default | None | | x |
| 13. | | | | Default | None | | x |
| 14. | | | | Default | None | | x |
| 15. | | | | Default | None | | x |
| 16. | | | | Default | None | | x |
| 17. | | | | Default | None | | x |
| 18. | | | | Default | None | | x |
| 19. | | | | Default | None | | x |
| 20. | | | | Default | None | | x |

<< 1-20 | 21-40 | 41-60 >> Next >>

Status: v --- Active, x --- Inactive, ? --- Empty

按任何一個索引標號進入下一個設定頁面。

VoIP >> DialPlan Setup

Phone Book Index No. 1

☑ Enable

| | |
|---|---|
| Phone Number | 1 |
| Display Name | Polly |
| SIP URL | 1112 @ fwd.pulver.com |
| Dial Out Account | Default |
| Loop through | None |
| Backup Phone Number | |

OK Clear Cancel

**啓用** 勾選此方塊啓用此號碼。

**電話號碼** 此索引編號的快速撥號號碼，任何號碼都可以使用，範圍是數字 **0-9** 以及*。

**顯示名稱** 您想要在朋友的電話螢幕上顯示出來的名稱，可讓您的朋友容易知道是誰打的電話。

**SIP URL** 請輸入朋友的 SIP 位址。

## 數字對應設定

爲了使用者的方便，本頁允許使用者以新號碼來編輯 SIP 帳號的前置號碼，或是取代該號碼等等，這個設定可以提供用戶一個透過 VoIP 介面快速且簡單的撥號方式。

VoIP >> DialPlan Setup

**Digit Map Setup**

| # | Enable | Prefix Number | Mode | OP Number | Min Len | Max Len | Interface |
|---|---|---|---|---|---|---|---|
| 1 | ☑ | 03 | Replace | 8863 | 7 | 9 | PSTN |
| 2 | ☑ | 886 | Strip | 886 | 8 | 10 | PSTN |
| 3 | ☐ | | None | | 0 | 0 | PSTN |
| 4 | ☐ | | None | | 0 | 0 | PSTN |
| 5 | ☐ | | None | | 0 | 0 | PSTN |
| 6 | ☐ | | None | | 0 | 0 | PSTN |
| 7 | ☐ | | None | | 0 | 0 | PSTN |
| 8 | ☐ | | None | | 0 | 0 | PSTN |
| 9 | ☐ | | None | | 0 | 0 | PSTN |
| 10 | ☐ | | None | | 0 | 0 | PSTN |
| 11 | ☐ | | None | | 0 | 0 | PSTN |
| 12 | ☐ | | None | | 0 | 0 | PSTN |
| 13 | ☐ | | None | | 0 | 0 | PSTN |
| 14 | ☐ | | None | | 0 | 0 | PSTN |
| 15 | ☐ | | None | | 0 | 0 | PSTN |
| 16 | ☐ | | None | | 0 | 0 | PSTN |
| 17 | ☐ | | None | | 0 | 0 | PSTN |
| 18 | ☐ | | None | | 0 | 0 | PSTN |
| 19 | ☐ | | None | | 0 | 0 | PSTN |
| 20 | ☐ | | None | | 0 | 0 | PSTN |

**Note:** Min Len and Max Len should be between 0~25.

OK Cancel

**啓用** 按此方塊啓動此功能。

**前置號碼** 此處所設定的號碼可用來新增，取代變更之號碼。

**模式** **無** – 無動作。
**新增** -當您選擇此模式時，變更號碼將會增加前置號碼於前面，並藉由選定的 VoIP 介面撥出。
**卸除** -當您選擇此模式時，變更號碼將會被刪除。
**取代**- 當您選擇此模式時，透過指定的 VoIP 介面之變更號碼將會被前置號碼所取代

Mode

Replace
- None
- Add
- Strip
- Replace

**變更號碼** 您在此處所輸入的號碼是您想要執行特殊功用的帳號前半部份(依據選擇的模式而定)。

**最小長度** 設定撥號的最小長度以套用前置號碼之設定，參考上圖所示，如果號碼介於 7 和 9，那麼該號碼可以就能套用此處所設定的前置號碼設定。

**最大長度** 設定撥號的最大長度以套用前置號碼之設定。

**介面** 請自預設的六組 SIP 帳號中選擇一個您想要啓動前置號碼設定的介面。

## 4.12.2 SIP 帳號

在此頁面中，您可以調整自己的 SIP 設定，當您申請一個帳號時，您的 ISP 服務供應商會給您一個帳號名稱或是使用者名稱、SIP 登錄者、代理人和網域名稱(最後三種在某些條件下，有可能是完全相同的)，您可以告訴您的成員有關您的 SIP 位址，表示法為**帳號名稱@網域名稱**。

當路由器打開時，將以使用帳號名稱@網域名稱來登錄，之後，您的電話將由 SIP 代理者以帳號名稱@網域名稱傳送至目的地作為辨識之用。

VoIP >> SIP Accounts

SIP Accounts List [Refresh]

| Index | Profile | Domain/Realm | Proxy | Account Name | Ring Port | Status |
|---|---|---|---|---|---|---|
| 1 | | | | --- | ☐Phone1 ☐Phone2 | - |
| 2 | | | | --- | ☐Phone1 ☐Phone2 | - |
| 3 | | | | --- | ☐Phone1 ☐Phone2 | - |
| 4 | | | | --- | ☐Phone1 ☐Phone2 | - |
| 5 | | | | --- | ☐Phone1 ☐Phone2 | - |
| 6 | | | | --- | ☐Phone1 ☐Phone2 | - |

R: success registered on SIP server
-: fail to register on SIP server

NAT Traversal Setting

| | |
|---|---|
| STUN Server: | |
| External IP: | |
| SIP PING Interval: | 150 sec |

[OK]

**索引** 按此鈕進入下一層設定頁面設定 SIP 帳號。

**設定檔** 顯示帳號的設定檔名稱。

**網域** 顯示 SIP 註冊伺服器的網域名稱或是 IP 位址。

**伺服器** 顯示 SIP 伺服器的網域名稱或是 IP 位址。

**帳號名稱** 顯示@前面的 SIP 位址帳號名稱。

**振鈴通訊埠** 指定接收電話時由哪一個通訊埠響鈴。

**STUN 伺服器** 輸入 STUN 伺服器的 IP 位址或是網域。

**外部 IP** 輸入閘道 IP 位址。

**SIP PING 間隔** 預設值為 150 秒，對 Nortel 伺服器而言這項設定是相當有用的。

**狀態** 顯示相關 SIP 帳號的狀態，**R** 表示此帳號已註冊成功，**–** 表示尚未成功註冊。

VoIP >> SIP Accounts

SIP Account Index No. 1

| | |
|---|---|
| Profile Name | (11 char max.) |
| Register | No ☐ Call without Registration |
| SIP Port | 5060 |
| Domain/Realm | (63 char max.) |
| Proxy | (63 char max.) |
| ☐ Act as outbound proxy | |
| Display Name | (23 char max.) |
| Account Number/Name | --- (63 char max.) |
| ☐ Authentication ID | (63 char max.) |
| Password | (63 char max.) |
| Expiry Time | 1 hour 3600 sec |
| NAT Traversal Support | None |
| Ring Port | ☐ Phone 1 ☐ Phone 2 |
| Ring Pattern | 1 |

OK Cancel

**設定檔名稱** 指定一個名稱作爲辨識之用，您可以使用與網域類似的名稱，例如網域名稱爲 *draytel.org*,您就可以在本區中設定 *draytel-1*。

**由此註冊** 指定您申請註冊時所透過的介面爲何，如果您不想註冊個人資料而直接使用 VoIP 撥號功能，請選擇**無**。某些 SIP 伺服器允許使用者不須登錄即可使用 VoIP 功能，針對這類伺服器，請您選擇**自動**，系統將爲您選擇最佳方式作爲 VoIP 撥號之用。

**IP 通訊埠** 通訊埠號用來傳送/接收 SIP 訊息以建立通訊，雖然預設值爲 5060，您仍可將之變更爲其他數字。不過在這種情形下，還需要對方也同時變更爲相同的數字才行。

**網域** 輸入註冊 SIP 伺服器的網域名稱或 IP 位址。

**伺服器** 您可以輸入 SIP 代理伺服器的 IP 位址(或網域名稱如 iptel.org)，所有在上述的**網域**區域中指定的訊息來說 Vigor 路由器將之傳送至代理者，由代理者來轉送此訊息。您可以在網域名稱後面輸入通訊埠號，指定該埠號爲資料傳輸的目的地 (例如 nat.draytel.org**:5065)。**

**以對外伺服器之身份來運作** 勾選此方塊以啓用伺服器成爲對外伺服器。

**顯示名稱** 您想要在朋友的電話顯示螢幕上出現的名稱。

**帳號名稱/號碼** 輸入 SIP 位址的帳號名稱，例如@之前的文字。

**驗證 ID 身分** 勾選此方塊啓用此功能並輸入名稱或號碼供 SIP 驗證，如果設定值與帳戶名稱相同，您就不必勾選此方塊另設數值。

**密碼** 當您以 SIP 服務註冊時所需提供的密碼。

**有效時間** 為 SIP 伺服器提保存使用者註冊帳號的有效時間。在到期之前，路由器將會再次傳送另一個註冊需求給予 SIP 登錄伺服器。

**NAT 穿透** 如果路由器(寬頻路由器)是透過其他裝置連接上網際網路，您就必須設定此功能。

NAT Traversal Support: None / Stun / Manual / Nortel

**無 –**.關閉此功能。

**Stun** –若路由器支援 Stun 伺服器，請選擇此項目。

**手動** –若您想要指定外部 IP 位址作為 NAT transversal 支援，請選擇此項目。

**Nortel** – 如果軟體支援 nortel 方案，您可以選擇此項目。

**振鈴通訊埠** 設定 VoIP 1,VoIP 2 作為 SIP 帳號的預設振鈴通訊埠。

**振鈴樣式** **選擇** VoIP 電話的振鈴樣式。

Ring Pattern: 1 / 2 / 3 / 4 / 5 / 6

## 4.12.3 電話設定

本頁讓使用者得以個別設定 Phone 1 和 Phone 2 。

VoIP >> Phone Settings

Phone List

| Index | Port | Call Feature | Codec | Tone | Gain (Mic/Speaker) | Default SIP Account | DTMF Relay |
|---|---|---|---|---|---|---|---|
| 1 | Phone1 | CW,CT, | G.729A/B | User Defined | 5/5 | | InBand |
| 2 | Phone2 | CW,CT, | G.729A/B | User Defined | 5/5 | | InBand |

RTP

☐ Symmetric RTP

Dynamic RTP Port Start: 10050

Dynamic RTP Port End: 15000

RTP TOS: IP precedence 5 | 10100000

OK

**電話清單**

**通訊埠 –** 有種通訊埠類型提供給您選擇。
**通話功能** – 這個欄位簡單描述此通電話的功能供使用者參考。
**Codec –** 每個通訊埠的預設 Codec 設定都會顯示在本區，您可以按索引號碼變更每個電話通訊埠的設定。
**音調** – 顯示進階頁面所設定的音調值。
**音量** - 顯示進階頁面中 Mic/Speaker 的音量設定。
**預設 SIP 帳號** – "draytel_1" 是預設的 SIP 帳號，您可按索引下方的編號變更 SIP 帳號設定。
**DTMF Relay** –顯示進階頁面中所設定的 DTMF 模式。

**RTP**

**Symmetric RTP –** 勾選此方塊啓用此功能。若要讓資料傳輸能在本機路由器與遠端路由器之間暢行無阻而不至於因 IP 漏失而誤導的情形發生，請您勾選此方塊解決這個問題。
**RTP 通訊埠起點** - 指定 RTP 之通訊埠起點，預設值爲 10050。
**RTP 通訊埠終點** - 指定 RTP 之通訊埠終點，預設值爲 15000。
**RTP TOS** –此項可決定 VoIP 封包的等級，請使用下拉式選項選擇其中一種。

Manual
IP precedence 1
IP precedence 2
IP precedence 3
IP precedence 4
IP precedence 5
IP precedence 6
IP precedence 7
AF Class1 (Low Drop)
AF Class1 (Medium Drop)
AF Class1 (High Drop)
AF Class2 (Low Drop)
AF Class2 (Medium Drop)
AF Class2 (High Drop)
AF Class3 (Low Drop)
AF Class3 (Medium Drop)
AF Class3 (High Drop)
AF Class4 (Low Drop)
AF Class4 (Medium Drop)
AF Class4 (High Drop)
EF Class

RTP TOS Manual

## Phone Port 細節設定

請按索引欄位下方的 1 或 2 連結進入下面的設定頁面。

VoIP >> Phone Settings

Phone1

Call Feature

Hotline

Session Timer 90 sec

Call Forwarding Disable

SIP URL

Time Out 30 sec

DND(Do Not Disturb) Mode

Index(1-15) in Schedule Setup:

Note: Action and Idle Timeout settings will be ignored.

Index(1-60) in Phone Book as Exception List:

CLIR (hide caller ID)

Call Waiting

Call Transfer

Codecs

Prefer Codec G.729A/B (8Kbps)

Single Codec

Packet Size 20ms

Voice Active Detector Off

Default SIP Account

Play dial tone only when account registered

OK Cancel Advanced

**熱線** 勾選此方塊啓用此功能，請在本區輸入 SIP URL 讓系統在您拿起話機後自動撥號。

**連線計數器** 勾選此方塊啓用此功能，您在本區所設定的限制時間內如果沒有任何回應，連線電話將會自動關閉。

**指定轉接** 共有四種選項可以選擇，**停用**可關閉此功能，**永遠**則表示來電會一直轉接到 SIP URL 上，**忙線**則表示來電只在本機忙碌時轉接到 SIP URL，**沒回應**則表示來電若未收到任何回應，電話都會在切斷時轉接到 SIP URL 上。

Disable

Disable
Always
Busy
No Answer

**SIP URL** – 請輸入 SIP URL (例如 aaa@draytel.org 或 abc@iptel.org) 做爲轉送電話的終點。

**逾時** – 設定電話轉接的逾時現制，預設值爲 30 秒。

**DND (勿干擾)** 設定一段和平時間不受任何 VoIP 來電的干擾。在此期間，撥號進來的人會聽到忙線的聲音，而本機用戶則聽不到任何電話鈴聲。

**索引 (1-15) 於排程設定... -** E 依照事先設定完成之排程，在此輸入排程計畫的索引編號以控制勿打擾模式。詳細設定請參考**排程**一節。

**索引(1-60) 於電話簿 -** 輸入例外電話於此方塊內，列於此之電話不受勿干擾的限制。詳細設定請參考**電話簿**一節。

**話中插接** 勾選此方塊啓用此功能，提示聲音將會出現以告知使用者有電話在等待。

| | |
|---|---|
| **電話轉接** | 勾選此方塊啓用此功能，按轉接鍵轉接另一通電話，當電話連線成功時，掛上電話。此時另外二方就可直接溝通。 |
| **偏好 Codec** | 有五種不同的 CODEC 供您選擇，但真正被使用的 CODEC 在通訊建立前是和對方共同商議而得。預設的 CODEC 是 G.729A/B，它佔據較少的頻寬但是卻仍擁有良好的聲音品質，如果您想要使用 G.711，您最好具有至少 256Kbps 的上傳速率。<br>Prefer Codec: G.711A (64Kbps) / G.711MU (64Kbps) / G.711A (64Kbps) / G.729A/B (8Kbps) / G.723 (6.4kbps) / G.726_32 (32kbps)<br>**單一 Codec** - 如果勾選此方塊，只有選定的 Codec 會被路由器套用。<br>**語音資料長度** - 資料總數包含單一封包(10, 20, 30, 40, 50 和 60)，預設值為 20ms，表示資料封包含 20ms 聲音資訊。<br>Packet Size: 20ms / 10ms / 20ms / 30ms / 40ms / 50ms / 60ms<br>**語音活動偵測器(AVD) -** 選擇**開啓**啓動此項功能，以檢測使用者是否正在交談。如果安靜無聲，路由器將採取行動節省頻寬的使用。<br>Voice Active Detector: Off / Off / On |
| **預設 SIP 帳號** | 您可以設定 SIP 帳號(最多 6 組)，請使用下拉式清單選擇其中一組作為預設帳號。<br>**當帳號已經註冊時請使用撥號音** - 勾選此方塊啓用此功能。 |

此外，您也可以按**進階**按鈕進入深一層的設定。此項設定是為了符合路由器安裝所在地區的電信習慣而提供，錯誤音調設定可能會造成使用者的不便。關於設定話機的聲音型態，方法很簡單，只要選擇適當的區域讓系統自動尋找事先設定的音調設定和呼叫 ID 類型，或是您也可選擇使用者自訂，然後以手動方式調整音調，TOn1, TOff1, TOn2 和 TOff2 表示音調型態的韻律，TOn1 和 TOn2 表示開啓聲音；TOff1 和 TOff2 則表示關閉聲音。

VoIP >> Phone Settings

Advance Settings >> Phone1

Tone Settings

Region: User Defined Caller ID Type: FSK_ETSI

| | Low Freq (Hz) | High Freq (Hz) | T on 1 (msec) | T off 1 (msec) | T on 2 (msec) | T off 2 (msec) |
|---|---|---|---|---|---|---|
| Dial tone | 350 | 440 | 0 | 0 | 0 | 0 |
| Ringing tone | 400 | 450 | 400 | 200 | 400 | 2000 |
| Busy tone | 400 | 0 | 375 | 375 | 0 | 0 |
| Congestion tone | 0 | 0 | 0 | 0 | 0 | 0 |

Volume Gain

Mic Gain(1-10): 5

Speaker Gain(1-10): 5

DTMF

DTMF Mode: InBand

Payload Type(RFC2833): 101

MISC

Dial Tone Power Level (1 - 50): 27

Ring Frequency (10 - 50HZ): 25

OK Cancel

**地區** 選擇您目前所處地區，**來電顯示類型**、**撥號音**、**響鈴音**、**忙線音**和**系統擁塞音**都會自動顯示在本頁面上。如果您無法找到適合的地區，請您選擇**使用者自訂**，再自行輸入頁面所需的各式資料。

Tone Settings

Region: User Defined

User Defined
UK
US
Denmark
Italy
Germany
Netherlands
Portugal
Sweden
Australia
Slovenia
Czech
Slovakia
Hungary
Switzerland

您也可以是個人需要指定各個區域內容，建議您採用預設值作爲 VoIP 通訊之用。

**來電顯示類型** 此處提供數種標準，以便在電話機面板上顯示來電者的身分，請依照路由器安裝所在地區選擇適合的類型，如果您不知道話機究竟支援哪種標準，請直接採用預設值。

**音量控制** 請輸入 1- 10 以設定麥克風的音量，數字越大聲音越大。

**雜項** **撥號音量控制** -此項設定用來調整撥號的音量大小，數字越小音量越大，建議使用預設值。

**振鈴聲頻率** 此項設定用來驅動鈴聲的頻率，建議使用預設值。

**DTMF**

**DTMF 模式**

***InBand* -** 當您按壓電話上的鍵盤時，路由器將會直接以聲音模式傳送 DTMF 音調。

***OutBand* -** 路由器將會抓取您所按壓的鍵盤號碼然後以數位格式傳送至另一端；接收者將會依照所接收的數位格式來產生音調。這個功能在網路擁塞的情形下是很有用處的，因爲它仍可保持 *DTMF 音調的準確度。*

***SIP 資訊*-**路由器將抓取 DTMF 音調然後以 SIP 訊息轉送給遠端用戶。

DTMF mode: InBand

- InBand
- OutBand ( RFC2833)
- SIP INFO (cisco format)
- SIP INFO (nortel format)

**Payload 類型 (rfc2833) -** 請自 96 至 127 中選擇一個數字，預設值爲 101，此項設定只對 OutBand (RFC2833)模式有效。

## 4.12.4 狀態

在 VoIP 撥號狀態下，您可以看見 VoIP 1 和 VoIP 2 的 codec、連線情形和其他重要的撥號狀態資料。

VoIP >> Status

Status — Refresh Seconds: 10 — Refresh

| Port | Status | Codec | PeerID | Elapse (hh:mm:ss) | Tx Pkts | Rx Pkts | Rx Losts | Rx Jitter (ms) | In Calls | Out Calls | Miss Calls | Speaker Gain |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Phone1 | IDLE | | | 00:00:00 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 5 |
| Phone2 | IDLE | | | 00:00:00 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 5 |

Log

| Date (mm-dd-yyyy) | Time (hh:mm:ss) | Duration (hh:mm:ss) | In/Out/Miss | Account ID | Peer ID |
|---|---|---|---|---|---|
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |
| 00-00- 0 | 00:00:00 | 00:00:00 | - | - | |

**更新間隔秒數** 指定更新的間隔秒數以取得最新的 VoIP 撥號資訊，當按下**更新頁面**按鈕時，頁面資訊將會立即更新。

更新間隔秒數: 10

- 5
- 10
- 30

**通訊埠** 顯示目前 VoIP 電話的連線通訊埠。

| | |
|---|---|
| **狀態** | 顯示 VoIP 連線狀態。<br>**IDLE -**表示 VoIP 功能正處於閒置狀態。<br>**HANG_UP -**表示連線並未建立(忙線音調)。<br>**CONNECTING -**表示用戶正撥出號碼中。<br>**WAIT_ANS -**表示已連線並等待遠端用戶的回答。<br>**ALERTING -**表示有來電。<br>**ACTIVE-**表示 VoIP 連線啓動。 |
| **Codec** | 表示目前頻道所利用的聲音 codec。 |
| **對方 ID** | 撥進或撥出之對方 ID (格式可以是 IP 位址或是網域名稱)。 |
| **經過時間** | 通話時間以秒數計算。 |
| **傳送封包數** | 在連線中全部的傳送封包數量。 |
| **接收封包數** | 在連線中全部的接收封包數量。 |
| **漏失接收封包** | 在連線中漏失的全部封包。 |
| **接收抖動** | 接收聲音封包抖動狀態。 |
| **來電** | 已接來電總數。 |
| **撥出電話** | 撥出電話總數。 |
| **接聽音量** | 電話音量大小。 |
| **記錄** | 顯示 VoIP 電話紀錄。 |

## 4.13 無線區域網路設定

注意: 本節所提供的資訊僅針對 *n* 系列機型。

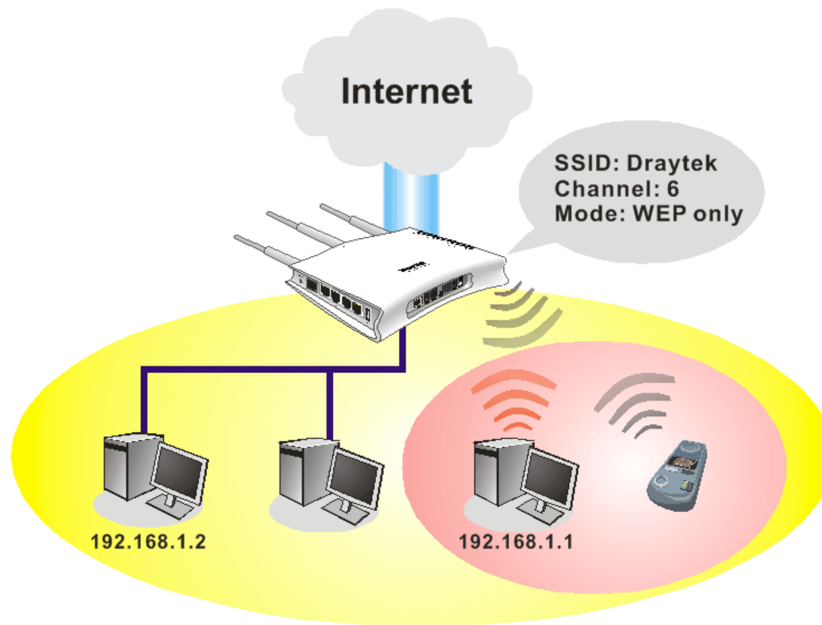
### 4.13.1 基本觀念

在最近幾年無線通訊的市場有了極大的成長，無線技術線在到達了或說是有能力到達地球表面上的每一個點，數以百萬的人們每天透過無線通訊產品彼此交換資訊，Vigor G 系列路由器，又稱爲 Vigor 無線路由器，被設計成爲一個適合小型辦公室/家庭需要的路由器，擁有最大的彈性與效率，任何一個被授權的人，都可以攜帶內建的無線區域網路用戶端 PDA 或是筆記型電腦，進入會議室開會，因而不需擺放一堆亂七八糟的纜線或是到處鑽孔以便連線。無線區域網路機動性高，因此無線區域網路使用者可以同時存取所有區域網路中的工具，以及遨遊網際網路，好比是以有線網路連接的一樣。

Vigor 無線路由器皆配有與標準 IEEE 802.11g 通訊協定相容之無線區域網路介面，爲了進一步提高其效能，Vigor 路由器也承載了進階無線技術 Super G ™ 以便將速率提升至 108 Mbps*，因此在最後您可以非常順利的享受流暢的音樂與影像。

> **注意**：*資料的實際總處理能力會依照網路條件和環境因素而改變，如網路流量、網路費用以及建造材料。

在無線網路的基礎建設模式(Infrastructure Mode)中，Vigor 無線路由器扮演著無線網路基地台(AP)的角色，可連接很多的無線用戶端或是無線用戶站(STA)，所有的用戶站透過路由器，都可分享相同的網際網路連線。**基本設定**可讓您針對無線網路所需的訊息包含 SSID、頻道等項目做基本的配置。




## Multiple SSIDs

### 安全防護概要

**即時硬體加密:** Vigor 路由器配有 AES 加密引擎，因此可以採用最高級的保護措施，在不影響使用者的習慣之下，對資料達成保護效果。

**完整的安全性標準選項:** 爲了確保無線通訊的安全性與私密性，提供數種市場上常見的無線安全標準。

有線對應隱私權(Wired Equivalent Privacy, WEP)是一種傳統的方法，使用 64-bit 或是 128-bit 金鑰透過無線收發裝置來加密每個資料訊框。通常無線基地台會事先配置一組含四個金鑰的設定，然後使用其中一個金鑰與每個無線用戶端通訊聯絡。

Wi-Fi 保護存取協定(Wi-Fi Protected Access, WPA)是工業上最佔優勢的安全機制，可分成二大類：WPA-personal 或稱爲 WPA Pre-Share Key (WPA/PSK)以及 WPA-Enterprise 又稱爲 WPA/802.1x。

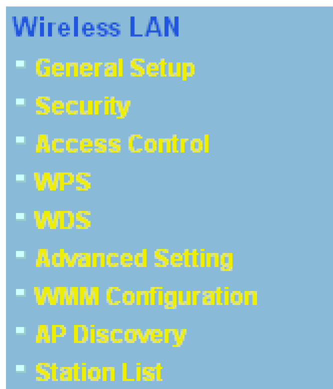
在 WPA-Personal 機制中，會應用一個事先定義的金鑰來加密傳輸中的資料，WPA 採用 Temporal Key Integrity Protocol (TKIP) 加密資料而 WPA2 則是採用 AES，WPA-Enterprise 不只結合加密也還涵括驗證功能。

由於 WEP 已被證明是有弱點的，您可以考慮使用 WPA 作爲安全連線之用。您應該按照所需來選擇適當的安全機制，不論您選擇哪一種安全防護措施，它們都可以全方位的加強您無線網路上之資料保護以及/或是機密性。Vigor 無線路由器是相當具有彈性的，且能同時以 WEP 和 WPA 支援多種安全連線。

**分隔無線與有線區域網路 - 無線區域網路隔離**可使您自有線區域網路中，分隔出無線區域網路以便隔離或是限制存取。隔離代表著雙方彼此都無法存取對方的資料，欲詳細說明商業用途之範例，您可以爲訪客設定一個無線區域網路，讓他們只能連接到網際網路而不必擔心洩露機密資訊。更彈性的作法是，您可以新增 MAC 位址的過濾器來區隔有線網路之單一使用者的存取行爲。

**管理無線用戶端 - 無線用戶端列表**顯示無線網路中全部的無線用戶端以及連接狀態。

以下爲**無線區域網路**下的功能項目：




## 4.13.2 基本設定

按下**一般設定**連結，新的網頁即會開啓，您可以設定 SSID 和無線頻道資訊，請參考下圖：

Wireless LAN >> General Setup

General Setting ( IEEE 802.11 )

☑ Enable Wireless LAN

Mode : Mixed(11b+11g+11n)

Index(1-15) in Schedule Setup: , , ,

Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored.

| | Enable | Hide SSID | SSID | Isolate LAN | Member |
|---|---|---|---|---|---|
| 1 | | ☐ | DrayTek | ☐ | ☐ |
| 2 | ☐ | ☐ | | ☐ | ☐ |
| 3 | ☐ | ☐ | | ☐ | ☐ |
| 4 | ☐ | ☐ | | ☐ | ☐ |

**Hide SSID:** Prevent SSID from being scanned.

**Isolate Member:**Wireless clients (stations) with the same SSID cannot access for each other.

**Isolate LAN:**Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.

Channel: Channel 6, 2437MHz Long Preamble: ☐

Long Preamble: necessary for some old 802.11 b devices only(lower performance)

Packet-OVERDRIVE™

☐ Tx Burst

**Note:**

The same technology must also be supported in clients to boost WLAN performance.

Rate Control

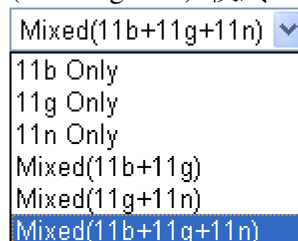
| | Enable | Upload | | Download | |
|---|---|---|---|---|---|
| SSID 1 | ☐ | 30000 | kbps | 30000 | kbps |
| SSID 2 | ☐ | 30000 | kbps | 30000 | kbps |
| SSID 3 | ☐ | 30000 | kbps | 30000 | kbps |
| SSID 4 | ☐ | 30000 | kbps | 30000 | kbps |

**Note:** range 100~50,000 kbps

OK Cancel

**啓用** 勾選此方塊啓動無線功能。

**模式** 請選擇一個適當的無線模式。目前路由器支援的協定有綜合( (11b+11g), 11g Only, 11b Only, 綜合( (11g+11n), 11n Only 及綜合( (11b+11g+11n)。 請選擇綜合(11b+11g+11n) 模式。

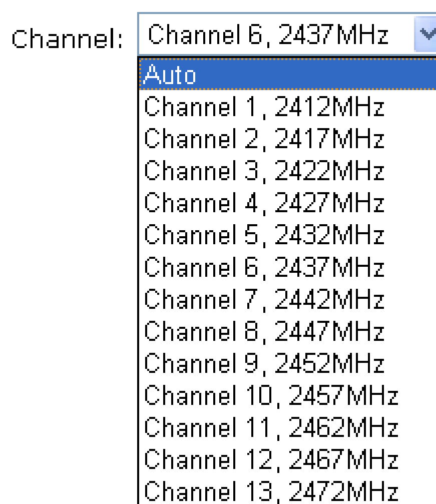



**索引(1-15)** 設定無線區域網路在特定的時間間隔中運作。您可以從**應用**的**排程設定**頁面上，自 15 個排程中選擇 4 個，本區預設值是空白的，表示無線功能是永遠可以運作的狀態。

**SSID** 預設的 SSID 值爲 **DrayTek**，建議您變更爲另一個特殊名稱。它是無線區域網路的身分辨識碼，SSID 可以是任何文字、數字或是各種特殊字元。

**隱藏 SSID** 勾選此方塊，防止他人得知 SSID 值，未知此路由器的 SSID 之無線用戶在搜尋網路時，看不到 Vigor 無線路由器的訊息。

**頻道** 無線區域網路的通道頻率，預設頻道是 6，如果選定的頻道受到嚴重的干擾的話，您可自行切換爲其他頻道。




**長封包標頭** 此選項用來定義 802.11 封包中同步區塊的長度，最新的無線網路以 56 bit 同步區來使用短封包標頭，而不是以 128 bit 同步區來使用長封包標頭。不過，一些原始 11b 無線網路裝置只有支援長封包標頭而已，因此如果您需要和此種裝置通訊溝通的話，請勾選此方塊。

### 4.13.3 安全性設定

擇**安全性設定**後，新的網頁將會出現，您可以在此頁面上調整 WEP 和 WPA 設定。

Wireless LAN >> Security Settings

SSID 1 | SSID 2 | SSID 3 | SSID 4

Mode: Disable

WPA:

Encryption Mode: TKIP

Pre-Shared Key(PSK): **************

Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".

WEP:

Encryption Mode: 64-Bit

Key 1 : **************

Key 2 : **************

Key 3 : **************

Key 4 : **************

For 64 bit WEP key
Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132".

For 128 bit WEP key
Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "0123456789abc" or "0x30313233343536373839414243".

OK | Cancel

**模式**

此一設定有數種模式可供您選擇。

Mode: Disable
Disable
WEP
WPA/PSK
WPA2/PSK
Mixed(WPA+WPA2)/PSK

Mode: Disable
Disable
WEP
WPA/PSK
WPA2/PSK
Mixed(WPA+WPA2)/PSK

**停用** - 關閉加密機制。

**WEP -** 只接受 WEP 用戶以及僅接受以 WEP 金鑰輸入的加密鑰匙。

**WPA/PSK -**接受 WPA 用戶，請在 PSK 中輸入加密金鑰。

**WPA2/PSK -**接受 WPA2 用戶，請在 PSK 中輸入加密金鑰。

**綜合 (WPA+ WPA2)/PSK –** 同時接受 WPA 與 WPA2 用戶，請在 PSK 中輸入加密金鑰。

**WPA**

WPA 可藉由金鑰加密每個來自無線網路的訊框，可在本區手動輸入 PSK，或是藉由 802.1x 驗證方式來自動加密。

**類型** – 選擇綜合 (WPA+WPA2) 或 WPA2。

**預先共用金鑰 (PSK)** - 輸入 **8~63** 個 ASCII 字元，像是 012345678（或是 64 個 16 進位數字，以 0x 開頭，如 0x321253abcde...）。

| | |
|---|---|
| **WEP** | **64-Bit** - 針對 64 位元的 WEP 金鑰，請輸入 5 個 ASCII 字元，像是 12345（或是 10 個 16 進位數字，以 0x 開頭，如 0x4142434445）。<br>**128-Bit** - 針對 128 位元的 WEP 金鑰，請輸入 13 個 ASCII 字元，像是 ABCDEFGHIJKLM（或是 16 個 16 進位數字，以 0x 開頭，如 0x4142434445）。<br>Encryption Mode: 64-Bit / 64-Bit / 128-Bit<br>所有的無線裝置都必須支援相同的 WEP 加密位元大小，並擁有相同的金鑰。這裡可以輸入四組金鑰，但一次只能選擇一組號碼來使用，這些金鑰可以 ASCII 文字或是 16 進位字元來輸入。請點選您想使用的金鑰組別。 |

## 4.13.4 連線控制

為了增加額外的無線存取安全性，連線控制頁面可讓您透過無線區域網路的用戶 MAC 位址來限制網路存取動作。只有設定有效的 MAC 位址得以存取無線區域網路介面，請選**連線控制**連結，開啓新的網頁，如同下圖所示，您即可在此頁面上編輯用戶端的 MAC 位址達到控制其存取權的目的。

Wireless LAN >> Access Control

Access Control

Enable Mac Address Filter

☐ SSID 1 ☐ SSID 2 ☐ SSID 3 ☐ SSID 4

MAC Address Filter

Index Attribute MAC Address

Client's MAC Address : __ : __ : __ : __ : __ : __

Attribute :

☐ s: Isolate the station from LAN

Add Delete Edit Cancel

OK Clear All

| | |
|---|---|
| **MAC 位址過濾** | 顯示之前編輯的全部 MAC 位址。 |
| **客戶端的 MAC 位址** | 請手動輸入無線用戶端的 MAC 位址。 |
| **特性** | **s -**勾選此項以便隔離無線用戶端之無線連線。 |
| **新增** | 新增新的 MAC 位址於清單上。 |
| **刪除** | 刪除清單中選定的 MAC 位址。 |
| **編輯** | 編輯清單中選定的 MAC 位址。 |

| | |
|---|---|
| **取消** | 放棄連線控制設定。 |
| **確定** | 按此鈕儲存連線控制清單。 |
| **全部清除** | 按此鈕儲存連線控制清單。 |

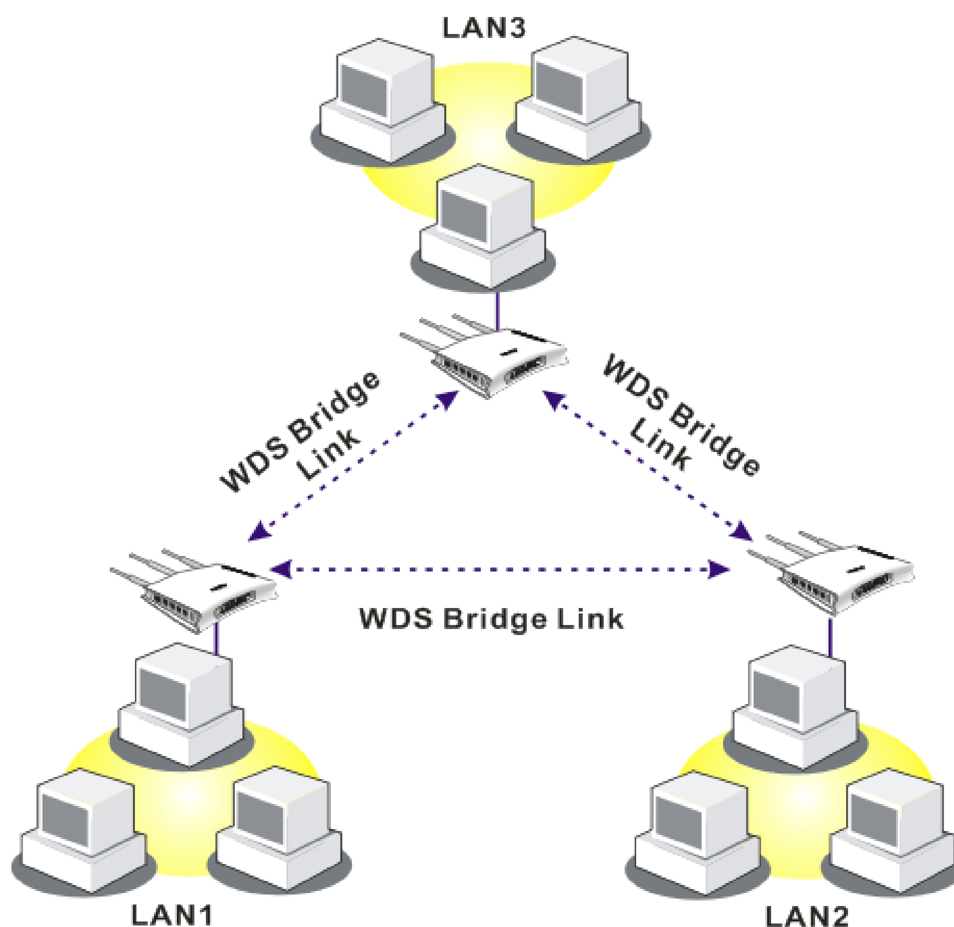
### 4.13.5 WPS

### 4.13.6 WDS

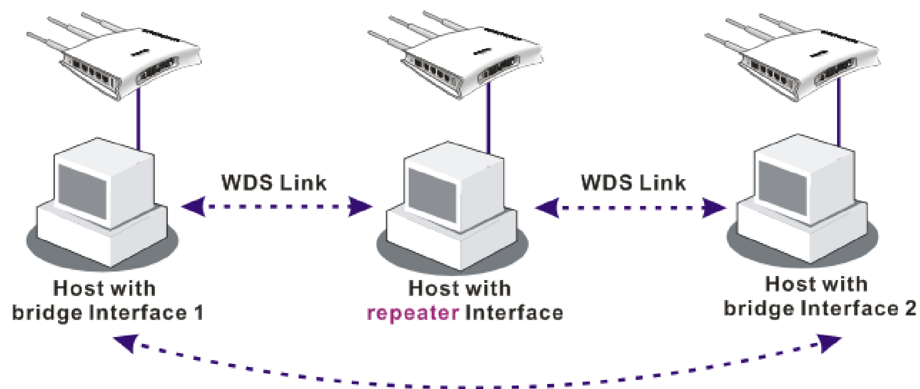
WDS 表示無線分派系統，是一個連結二個無線基地台的通訊協定，通常可以下列二種方式來應用。

- 提供二個區域網路間空中交流的橋樑
- 延長無線區域網路的涵蓋範圍

迎合以上的需要，路由器可應用二種 WDS 模式，一爲**橋接**一爲**中繼**，下圖顯示 WDS 橋接介面的功能：

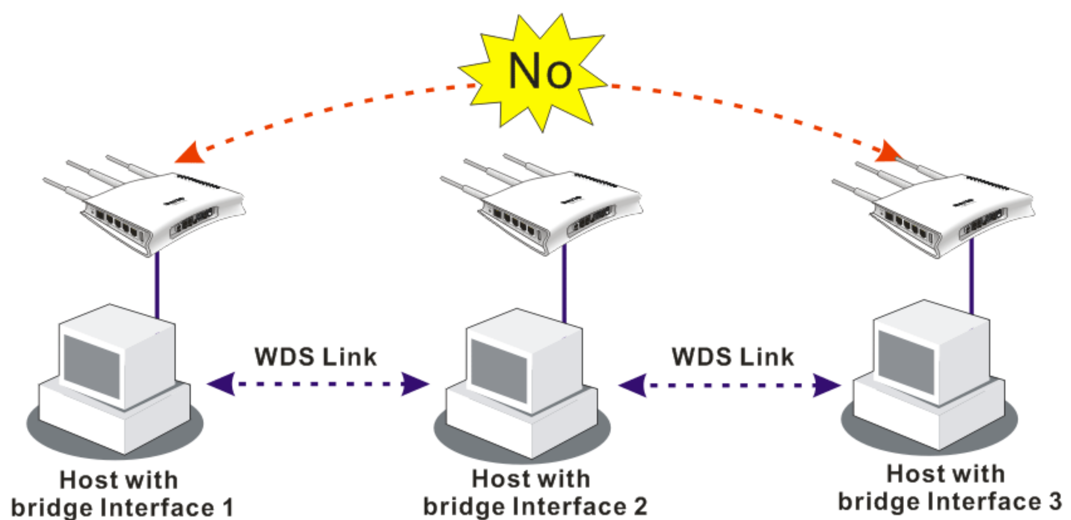



WDS-中繼模式的應用則描繪如下：




二種模式的主要不同點在於：**中繼**模式下，從一端 AP 過來的封包可以透過 WDS 連結再另一個 AP 上重複產生，WDS 連結傳送過來的封包只能轉送至本機有線或無線的主機。換言之，只有此模式能完成 WDS 到 WDS 封包轉送的工作

在下面這個例子當中，連接至橋接介面 1 或 3 的主機可以透過 WDS 連結與橋接介面 2 相連。不過連接至橋接 1 的主機無法透過橋接介面 2 與橋接介面 3 的主機相通。




按**無線區域網路**中的 **WDS** 功能以出現如下畫面：

Wireless LAN >> WDS Settings

WDS Settings | Set to Factory Default |

Mode: Bridge

Security:
Disable WEP Pre-shared Key

WEP:
Use the same WEP key set in Security Settings.

Pre-shared Key:
Type : TKIP
Key : **************

Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".

Bridge
Enable Peer MAC Address

Note: Disable unused links to get better performance.

Repeater
Enable Peer MAC Address

Access Point Function:
Enable Disable

Status:
Send "Hello" message to peers.

Link Status

Note: The status is valid only when the peer also supports this function.

OK Cancel

**模式** 選擇 WDS 設定模式，停用將無法啓用任何 WDS 設定；橋接模式乃是設計用來符合第一種實際之應用；**Repeater** 模式則是設計用來符合第二種實際之應用。

Disable
Disable
Bridge
Repeater

**安全性** 有三種安全性類型可選擇，停用、WEP 和預設共用金鑰。您在此處所選擇的設定將會使得 WEP 或是預設共用金鑰有效或是無效。請自三種中挑選出一種。

**WEP** 勾選此方塊使用**安全性設定**頁面中同樣的金鑰。如果您並未在**安全性設定**頁面中設定任何的金鑰，此方塊將暫時無法使用。

**預設共用金鑰** 輸入開頭爲“0x”之 8 ~ 63 個 ASCII 字元或是 64 的 16 進位的數字。

**橋接** 如果您選擇橋接做爲通訊模式，請在此區輸入對方的 MAC 位址，本頁可讓您一次輸入六個對方 MAC 位址。停用不使用的連結可以取得較好的執行效果，如果您想要啓動對方的 MAC 位址，記得輸入完成後勾選**啓用**方塊。

| | |
|---|---|
| **中繼** | 如果您選擇 Repeater 做為通訊模式，請在此區輸入對方的 MAC 位址，本頁可讓您一次輸入二個對方 MAC 位址。同樣的，如果您想要啓動對方的 MAC 位址，記得輸入完成後勾選**啓用**方塊。 |
| **無線基地台功能** | 按**啓用**讓路由器提供無線基地台的服務；按**停用**取消此功能。 |
| **狀態** | 允許使用者傳送招呼訊息給對方，然而則此功能僅在對方也支援時才有效用。 |

## 4.13.9 搜尋無線基地台

路由器可以掃描全部的頻道以及發現鄰近地區運作中的無線基地台，基於掃描的結果，使用者將會知道哪個頻道是可用的，此外它也可以用來發現 WDS 連結中的無線基地台，注意在掃描過程中(約 5 秒)，任何一台無線用戶都不可以連接上路由器。

本頁可用來掃描無線區域網路中的無線基地台的存在，不過只有與路由器相同頻道的無線基地台可以被發現，請按**掃描**按鈕尋找所有相連的無線基地台。

Wireless LAN >> Access Point Discovery

Access Point List

BSSID Channel SSID

Scan

See Statistics.

Note: During the scanning process (~5 seconds), no station is allowed to connect with the router.

Add to WDS Settings :

AP's MAC address : : : : :

Add to  Bridge  Repeater

| | |
|---|---|
| **掃描** | |
| **統計** | |
| **新增** | 如果您想要找到套用 WDS 設定的無線基地台，請在本頁底部輸入該 AP 的 MAC 位址，然後按**新增**，稍後該 MAC 位址即會加入 WDS 設定頁面中。 |

## 4.13.10 無線用戶端列表

**無線用戶端列表**提供您目前相連之無線用戶的狀態碼，下圖針對狀態碼提供了詳盡的解說，為了能有更方便的連線控制，您可以選擇一台 WLAN 用戶站然後選擇**新增到連線控制**，這樣就可以了

Wireless LAN >> Station List

Station List

| Status | MAC Address | Associated with |
| --- | --- | --- |

Refresh

**Status Codes :**
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.

Note: After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.

Add to Access Control :

Client's MAC address [ ] : [ ] : [ ] : [ ] : [ ] : [ ]

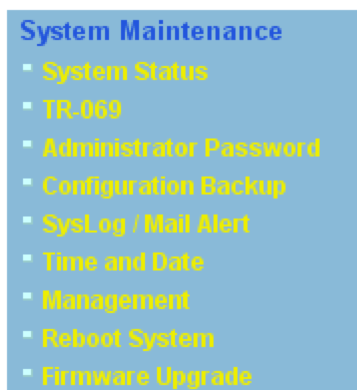
Add

| | |
| --- | --- |
| **更新頁面** | 按此鈕更新用戶端的 MAC 位址列表。 |
| **新增** | 按此鈕新增選定之 MAC 位址至**連線控制**。 |

## 4.14 系統維護

系統設定方面，有數種項目是使用者需要了解的：系統狀態、系統管理員密碼、備份組態、系統紀錄/郵件警示、時間設定、重啓系統及韌體升級等等。

下圖爲系統維護的主要設定功能。




### 4.12.1 系統狀態

系統狀態提供基本的網路設定，包含區域網路和 WAN 介面等資訊，同時您也可以獲得目前執行中的韌體版本或是韌體其他的相關資訊。

System Status

Model Name : Vigor2110 series
Firmware Version : 3.3.0_RC5
Build Date/Time : Feb 11 2009 14:25:46

| LAN | |
|---|---|
| MAC Address | : 00-50-7F-9A-32-70 |
| 1st IP Address | : 192.168.1.5 |
| 1st Subnet Mask | : 255.255.255.0 |
| DHCP Server | : Yes |
| DNS | : 172.16.3.18 |

| WAN | |
|---|---|
| Link Status | : Connected |
| MAC Address | : 00-50-7F-9A-32-71 |
| Connection | : DHCP Client |
| IP Address | : 192.168.5.26 |
| Default Gateway | : 192.168.5.1 |

| VoIP | | | |
|---|---|---|---|
| Port | Profile | Reg. | In/Out |
| Phone1 | | No | 0/0 |
| Phone2 | | No | 0/0 |

| Wireless LAN | |
|---|---|
| MAC Address | : 00-50-7f-9a-32-70 |
| Frequency Domain | : Europe |
| Firmware Version | : 1.8.1.0 |
| SSID | : DrayTek |

| | |
|---|---|
| **型號名稱** | 顯示路由器的型號名稱。 |
| **韌體版本** | 顯示路由器的韌體版本。 |
| **建立日期與時間** | 顯示目前韌體建立的日期與時間。 |
| ***LAN-------*** | |
| **MAC 位址** | 顯示區域網路介面的 MAC 位址。 |
| **第一個 IP 位址** | 顯示區域網路介面的 IP 位址。 |
| **第一個子網路遮罩** | 顯示區域網路介面的子網路遮罩位址。 |
| **DHCP 伺服器** | 顯示區域網路介面的 DHCP 伺服器目前的狀態。 |

| | |
|---|---|
| **DNS** | 顯示主要 DNS 的 IP 位址。 |
| ***WAN-------*** | |
| **連線狀態** | 顯示目前實體連線的狀態。 |
| **MAC 位址** | 顯示 WAN 介面的 MAC 位址。 |
| **IP 位址** | 顯示 WAN 介面的 IP 位址。 |
| **預設閘道** | 顯示預設閘道指定的 IP 位址。 |
| ***Wireless LAN-------*** | |
| **MAC 位址** | 顯示無線區域網路的 MAC 位址。 |
| **頻率網域** | 網域可以是歐洲(13 個可用頻道),美國(11 個可用頻道)，無線產品所支援之可用頻道在不同的國家下是不相同的。 |
| **韌體版本** | 表示配備 WLAN miniPCi 卡的詳細資訊，同時可以提供該卡相關的特徵訊息。 |
| **SSID** | 顯示路由器的 SSID。 |

## 4.14.3 系統管理員密碼

本頁允許您設定新的密碼。

System Maintenance >> Administrator Password Setup

Administrator Password

| | |
|---|---|
| Old Password | |
| New Password | |
| Confirm Password | |

OK

| | |
|---|---|
| **舊密碼** | 請輸入舊密碼，出廠預設值是空白的。 |
| **新密碼** | 請在本區輸入新密碼。 |
| **確認密碼** | 再次輸入新密碼以確認。 |

當您按下確定鍵後，登入視窗將會出現，請使用新的密碼以便再次存取網頁設定頁面。

## 4.14.4 設定備份

### 設定備份

請依照下列步驟備份您的路由器設定。

1. 在**系統維護**群組中按**設定備份**，您將可看見如下視窗。

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

Select a configuration file.

Browse..

Click Restore to upload the file.

Restore

Backup

Click Backup to download current running configurations as a file.

Backup Cancel

2. 按**備份**按鈕進入下一個對話盒，按**儲存**按鈕開啓另一個視窗以儲存設定。

檔案下載

是否要儲存這個檔案?

名稱: config.cfg

類型: 不明的檔案類型，3.00 KB

來自: 192.168.1.1

儲存(S) 取消

雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要儲存這個檔案。有什麼樣的風險?

3. 在**另存新檔**對話盒中，預設檔名爲 **config.cfg**，您也可以在此輸入不同的檔名。

另存新檔

儲存於(I): 桌面

我的文件

我的電腦

網路上的芳鄰

我最近的文件

桌面

我的文件

我的電腦

網路上的芳鄰

檔名(N): config

存檔類型(T): .cfg 文件

儲存(S)

取消

1. 按下**儲存**按鈕，設定將會以檔名 **config.cfg** 自動下載至電腦上。

上述範例是以 Windows 平台來完成，對於 **Mac** 或是 **Linux** 平台的用戶，螢幕上將會出現不一樣的視窗，但是備份的功能仍是有效的。

| **附註:**憑證備份須以另一種方式來儲存，備份設定並不包含憑證資訊。 |
|---|

**還原設定**

1. 在**系統維護**群組中按**設定備份**，您將可看見如下視窗。

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

Select a configuration file.

Browse..

Click Restore to upload the file.

Restore

Backup

Click Backup to download current running configurations as a file.

Backup Cancel

2. 按**瀏覽**按鈕選擇正確的設定檔案，以便上傳至路由器。
3. 按**還原**按鈕並等待數秒鐘，下述畫面出現即告訴您還原動作已成功。

## 4.14.5 Syslog/郵件警示設定

SysLog 在 Unix 系統中是很受歡迎的一種工具，如果要監視路由器的運作狀態，您可以執行 SysLog 程式擷取路由器上所有的活動。此依程式可以在本地電腦或是網際網路上任一遠端電腦上執行，此外 Vigor 路由器提供郵件警示功能，這樣 SysLog 訊息可以郵件方式打包寄給資訊管理人員。

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

| SysLog Access Setup | | Mail Alert Setup | |
|---|---|---|---|
| ☑ Enable | | ☐ Enable | Send a test e-mail |
| Server IP Address | | SMTP Server | |
| Destination Port | 514 | Mail To | |
| Enable syslog message: | | Return-Path | |
| ☑ Firewall Log | | ☐ Authentication | |
| ☑ VPN Log | | User Name | |
| ☑ User Access Log | | Password | |
| ☑ Call Log | | Enable E-Mail Alert: | |
| ☑ WAN Log | | ☑ DoS Attack | |
| ☑ Router/DSL information | | ☑ IM-P2P | |

OK Clear Cancel

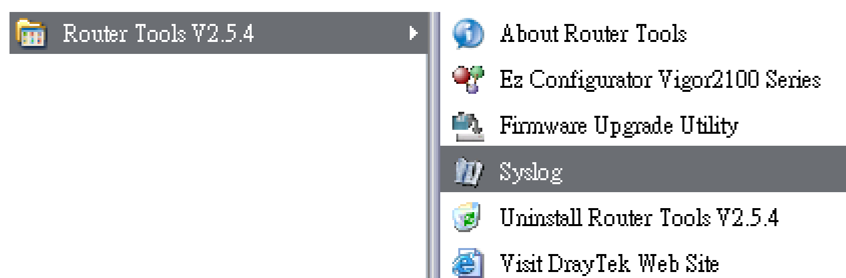
| | |
|---|---|
| **啓用** | 勾選**啓用**以啓動系統記錄服務功能/啓動郵件警示功能。 |
| **伺服器 IP 位址** | 指定全部系統紀錄訊息傳送前往目的地之 IP 位址。 |

| | |
|---|---|
| **目標通訊埠** | 指定全部系統紀錄訊息傳送前往目的地之通訊埠。 |
| **SMTP 伺服器** | 指定 SMTP 伺服器的 IP 位址，直接傳送來自 Vigor 路由器的郵件至收信人的信箱。 |
| **收件人** | 指定收信人信箱的郵件地址，全部的系統紀錄訊息將會自動傳送至此處。收信人可以是想要檢視或是分析系統紀錄訊息的管理人員。 |
| **回信地址** | 指定另一組信箱的郵件地址，接收因收信人信箱錯誤而造成發生失敗的所有回覆訊息。 |
| **驗證** | 當使用電子郵件應用程式，勾選此方塊可啓動驗證的功能。 |
| **使用者名稱** | 輸入驗證所需的使用者名稱。 |
| **密碼** | 輸入驗證所需的密碼。 |

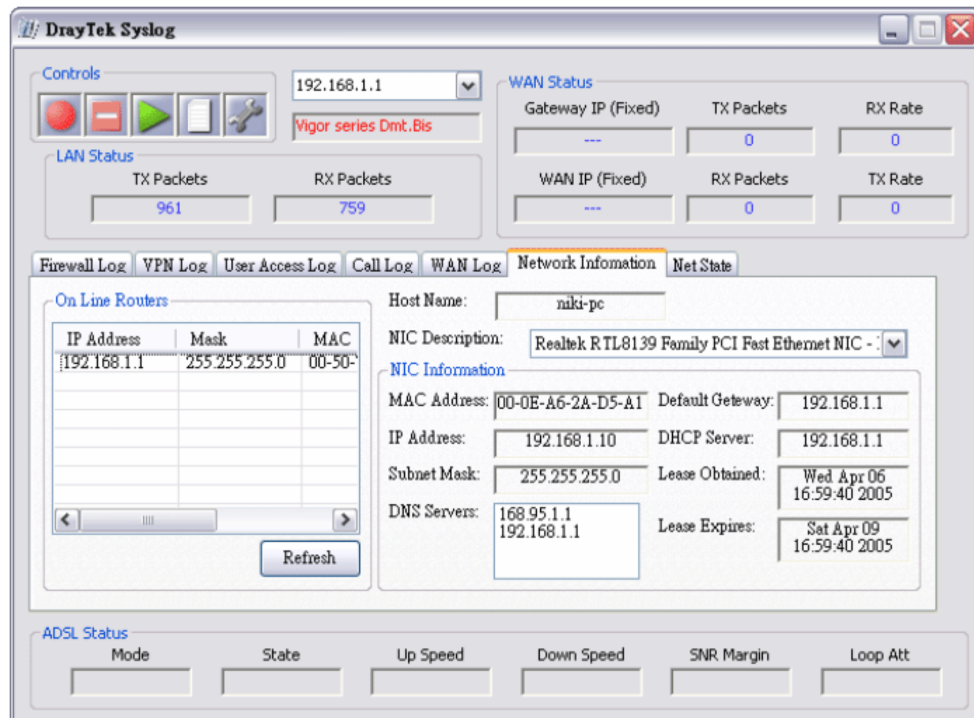
按**確定**儲存所有的設定。

如欲檢視系統紀錄，請依照下述步驟進行：

1. 請在伺服器 IP 地址中設定監視電腦的 IP 地址。
2. 安裝光碟片中 **Utility** 下的路由器工具，安裝完畢後，請自程式集選取 **Router Tools>>Syslog**。




3. 自 Syslog 畫面上，選擇您想要監視的路由器。請記住在網路資訊(**Network Information)**中，選擇用來連接路由器的網路交換器，否則您無法成功檢索來自路由器的資訊。




## 4.14.6 時間和日期

允許您指定自何處取得路由器時間。

**System Maintenance >> Time and Date**

**Time Information**

| Current System Time | 2000 Jan 2 Sun 3 : 31 : 21 | Inquire Time |
|---|---|---|

**Time Setup**

- ○ Use Browser Time
- ◉ Use Internet Time Client

| | |
|---|---|
| Server IP Address | pool.ntp.org |
| Time Zone | (GMT) Greenwich Mean Time : Dublin |
| Enable Daylight Saving | ☐ |
| Automatically Update Interval | 30 min |

OK Cancel

| | |
|---|---|
| **目前系統時間** | 按**取得時間**按鈕取得目前時間。 |
| **使用本台 PC 的時間** | 選擇此項以便採用遠端管理者電腦上的瀏覽器時間，作。 |
| **使用網際網路的時間伺服器** | 選擇此項以便自網際網路上的時間伺服器選擇所需的時間資訊。 |
| **時間協定** | 選擇適合本地的時間協定。 |
| **伺服器 IP 位址** | 輸入時間伺服器的 IP 地址。 |

| | |
|---|---|
| **時區** | 選擇路由器所在的時區。 |
| **啓動日光節約時間** | 勾選此方塊啓動日光節約時間，在某些地區，這個項目是很有用處的。 |
| **自動更新間隔** | 選定時間間隔以供 NTP 伺服器更新之用。 |

全部設定完成之後請按**確定**儲存目前的設定。

## 4.14.7 管理

本頁讓您管理存取控制、存取清單、通訊埠設定以及 SNMP 設定。例如管理存取控制時，埠號用來傳送/接收 SIP 訊息以便建立連線。

System Maintenance >> Management

Management Setup

Management Access Control

- [x] Allow management from the Internet
  - [ ] FTP Server
  - [x] HTTP Server
  - [x] HTTPS Server
  - [x] Telnet Server
  - [ ] SSH Server
- [x] Disable PING from the Internet

Access List

| List | IP | Subnet Mask |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |

Management Port Setup

(◉) User Define Ports ( ) Default Ports

| | | |
|---|---|---|
| Telnet Port | 23 | (Default: 23) |
| HTTP Port | 80 | (Default: 80) |
| HTTPS Port | 443 | (Default: 443) |
| FTP Port | 21 | (Default: 21) |
| SSH Port | 22 | (Default: 22) |

SNMP Setup

- [ ] Enable SNMP Agent

| | | |
|---|---|---|
| Get Community | public | |
| Set Community | private | |
| Manager Host IP | | |
| Trap Community | public | |
| Notification Host IP | | |
| Trap Timeout | 10 | seconds |

OK

| | |
|---|---|
| **允許從網路管理** | 勾選此方塊允許系統管理者自網際網路登入。系統提供數種不同的伺服器供您選擇作爲網路管理介面，請勾選所需的項目。 |
| **斷絕來自網際網路的 PING** | 勾選此方塊以退回所有來自網際網路的 PING 封包，考量到安全性問題，這項功能的預設值是啓動的。 |
| **存取清單** | 您可以指定系統管理者只能從指定的主機或是清單定義的網路上登入，您一次最多可定義三個 IP/子網路遮罩於此區域中。<br>**清單 IP** – 指定一個允許登入至路由器的 IP 地址。<br>**子網路遮罩** -代表允許登入至路由器的子網路遮罩。 |
| **預設通訊埠** | 勾選此項以使用標準埠號作爲 Telnet 和 HTTP 伺服器之用。 |
| **使用者定義通訊埠** | 勾選此項以指定使用者定義的埠號作爲 Telnet、HTTP 和 FTP 伺服器之用。 |

| | |
|---|---|
| **啓用 SNMP 代理程式** | 勾選此項以啓動此功能。 |
| **取得社群 (Get Community)** | 請輸入適當的文字以設定取得社群名稱，預設名稱為 **public。** |
| **設定社群 (Set Community)** | 請輸入適當的名稱以設定社群，預設名稱為 **private。** |
| **管理者主機 IP** | 設定一台主機做為管理者以便執行 SNMP 功能，請輸入 IP 位址指定特定主機。 |
| **封鎖社群(Trap Community)** | 輸入適當名稱設定封鎖社群，預設名稱為 **public。** |
| **通知主機 IP** | 設定主機的 IP 地址接收封鎖社群的資料。 |
| **封鎖逾時** | 預設值為 10 秒。 |

## 4.14.8 重啓路由器

網路設定可以用來重新啓動路由器，請自**系統維護**中按**重啓路由器**開啓如下頁面。

System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

- Using current configuration
- Using factory default configuration

OK

如果您想要使用目前的設定來重新啓動路由器，請勾選**使用目前組態**，然後按**確定**；如果要重設路由器設定回復成為預設值，請勾選**使用原廠預設組態**，然後按**確定**，路由器將會花 5 秒重新啓動系統。

**注意:**.當系統在您完成網頁設定並跳出**重啓路由器**網頁後，請務必按下**確定**以重新啓動路由器，這個動作可以確保系統的操作正常，且可避免未來發生不預期的錯誤。

## 4.14.9 韌體升級

在您更新路由器韌體之前，您必須先行安裝路由器工具。**韌體更新工作**即包含在此工具內，以下的網頁透過範例說明引導您更新韌體，注意此範例是在 Windows 操作系統下完成。

自居易網站或是 FTP 站下載最新的韌體版本，居易網站為 www.draytek.com，FTP 站則是 ftp.draytek.com。

請自**系統維護**選擇**韌體升級**以便啓動韌體更新工具。

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade

Select a firmware file.

[ ] Browse..

Click Upgrade to upload the file. Upgrade

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.3.0_RC5

Firmware Upgrade Procedures:

1. Click "OK" to start the TFTP server.
2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
3. Check that the firmware filename is correct.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is compelete, the TFTP server will automatically stop running.

Do you want to upgrade firmware ? OK

按**確定**，下述畫面將會出現，請先使用韌體更新工具完成更新。

System Maintenance >> Firmware Upgrade

TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

有關韌體更新的詳細資訊，請參考第四章。

## 4.15 自我診斷工具

自我診斷工具提供一個非常有效的方式，讓使用者能夠檢視或是診斷路由器的現況。以下為自我診斷的選單項目：




### 4.15.1 撥號觸發器

按**自我診斷工具**的**撥號觸發器**開啓網頁，網際網路連線(如 PPPoE)可由來源 IP 位址封包來觸發。

Diagnostics >> Dial-out Trigger

Dial-out Triggered Packet Header | Refresh |

HEX Format:

```
00 00 00 00 00 00-00 00 00 00 00 00-00 00

00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

Decoded Format:

```
0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)
```

| | |
|---|---|
| **已解碼格式** | 顯示來源 IP 位址、目標 IP 位址、通訊協定和封包的長度。 |
| **更新頁面** | 按此鈕重新載入本頁。 |

## 4.15.2 路由表

按**自我診斷工具**的**路由表**檢視路由器的路由表格，此表格可提供目前的 IP 路由資訊。

Diagnostics >> View Routing Table

Current Running Routing Table | Refresh |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
S~       192.168.10.0/    255.255.255.0 via 192.168.1.2,     LAN
C~        192.168.1.0/    255.255.255.0 is directly connected,     LAN
S~       211.100.88.0/    255.255.255.0 via 192.168.1.3,     LAN
```

| | |
|---|---|
| **更新頁面** | 按此鈕重新載入本頁。 |

## 4.15.3 ARP 快取表

按**自我診斷工具**的 **ARP 快取表**檢視路由器中 ARP(Address Resolution Protocol)快取的內容，此表格顯示乙太網路硬體位址(MAC 位址)和 IP 位址間的對應狀況。

Diagnostics >> View ARP Cache Table

Ethernet ARP Cache Table | Clear | Refresh |

```
IP Address          MAC Address          Netbios Name
192.168.1.1         00-50-7F-C2-80-20
192.168.1.10        00-0E-A6-2A-D5-A1     USER-6A0E182CE8
```

| | |
|---|---|
| **更新頁面** | 按此鈕重新載入本頁。 |
| **清除** | 按此連結清除整個表格。 |

## 4.15.4 DHCP 表

此工具提供指派 IP 位址的相關資訊，這項資訊對於診斷網路問題像是 IP 位址衝突等是很有幫助的。

按**自我診斷工具**，選擇 **DHCP 表**開啓相關網頁。

Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table | Refresh |

```
DHCP server: Running
Index    IP Address       MAC Address              Leased Time      HOST ID
```

**Index** 顯示連線項目編號。

**IP Address** 顯示路由器指派給特定電腦的 IP 位址。

**MAC Address** 顯示 DHCP 指派給特定電腦的 MAC 位址。

**Leased Time** 顯示指定電腦的租約時間。

**HOST ID** 顯示指定電腦的主機 ID 名稱。

**更新頁面** 按此鈕重新載入本頁。

## 4.15.5 NAT 連線數狀態表

按**自我診斷工具**，選擇 **NAT 連線數狀態表**開啓相關網頁。

Diagnostics >> NAT Sessions Table

NAT Active Sessions Table | Refresh |

```
-------------------------------------------------------------------------------
     Private IP :Port #Pseudo Port         Peer IP :Port  Interface
-------------------------------------------------------------------------------
```

**Private IP:Port** 本機電腦的 IP 位址和埠號。

**#Pseudo Port** 路由器為了執行 NAT 所使用的暫時通訊埠。

**Peer IP:Port** 遠端主機的目標 IP 位址與埠號。

**Interface** 顯示 WAN 連線的介面。

**更新** 按此鈕重新載入本頁。

### 4.15.6 Data Flow Monitor

### 資料流量監控

本頁顯示所監視的 IP 位址執行的過程，並在數秒的間隔後重新更新頁面，此處所列出的 IP 位址是在頻寬管理中設定完成的，在啓動資料流量監控之前，您必須啓動 IP 頻寬限制以及 IP 連線數限制。若沒有這麼做的話，系統會出現知會畫面提醒您先啓動相關設定。

按**自我診斷工具**，選擇**資料流量監控**開啓相關網頁。您可按下 IP 位址、**TX 速率**、**RX 速率**或是**連線數**來排列資料。

Diagnostics >> Data Flow Monitor

☑ Enable Data Flow Monitor

Refresh Seconds: 10 Page: 1 | Refresh |

| Index | IP Address | TX rate(Kbps) | RX rate(Kbps) | Sessions | Action |
|---|---|---|---|---|---|

Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.
2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.

**啓用資料流量監控** 勾選此方塊以啓動此功能。

**更新秒數** 使用下拉式選項選擇系統自動更新資料的間隔時間。

Refresh Seconds: 10
10
15
30

**更新頁面** 按此連結更新本頁。

**索引編號** 顯示資料流量的項目筆數。

**IP 位址** 顯示被監視裝置的 IP 位址。

**傳送速率 (kbps)** 顯示被監視裝置的傳送速率。

**接收速率 (kbps)** 顯示被監視裝置的接收速率。

**NAT 連線數** 顯示您在連線數限制網頁中所設定的連線數。

**動作** **封鎖** – 可以避免指定電腦在 5 分鐘內存取網際網路。

| ps) | Sessions | Action |
|---|---|---|
| | 7 | Block |

**解除** – 指定 IP 位址的裝置將在五分鐘內封鎖起來，剩餘時間將顯示在 NAT 連線數欄位中。

| | Sessions | Action |
|---|---|---|
| | blocked / 298 | Unblock |

## 4.15.7 Ping 自我診斷

按**自我診斷工具**，選擇 **Ping 自我診斷**開啓相關網頁。

Diagnostics >> Ping Diagnosis

Ping Diagnosis

Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".

Ping to: Host / IP (Host / IP, Gateway, DNS) IP Address: Run

Result | Clear |

**Ping 至** 使用下拉式清單選擇您想要 Ping 的目標。

**IP 位址** 輸入您想要 Ping 的主機/IP 上的 IP 位址。

**執行** 按此鈕啓動 Ping 作業，結果將會顯示在螢幕上。

**清除** 按此連結清除視窗上的結果。

## 4.15.8 追蹤路由

按下**診斷工具**，選擇**追蹤路由**開啓相關網頁。本頁允許您追蹤路由器至主機之間的路由情況，只要簡單的輸入主機的 IP 位址並按下執行按鈕，整個路由狀況都將顯示在螢幕上。

Diagnostics >> Trace Route

Trace Route

Protocol: ICMP (ICMP / UDP)

Host / IP Address: [ ] Run

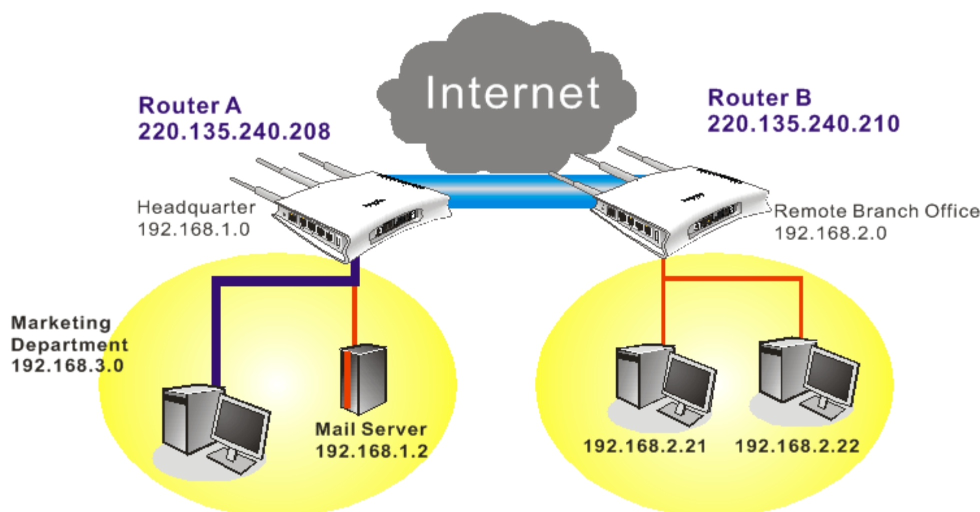
Result | Clear |

| | |
|---|---|
| **追蹤經由介面** | 使用下拉式清單選擇您想要經由其處來追蹤的 WAN 介面，或使用**不指定**讓路由器自動決定選擇哪一種介面。 |
| **主機/IP 位址** | 指明主機的 IP 位址。 |
| **執行** | 按此鈕開始路由追蹤動作。 |
| **清除** | 按此連結刪除視窗上的結果。 |

# 5 應用與範例

## 5.1 建立遠端辦公室與總公司之間的 LAN-to-LAN 連線

最常見的範例是例如遠端分公司與總公司之間的安全連線，依照下圖所顯示的網路結構，您可以遵循提供的步驟來建立 LAN-to-LAN 設定檔案，這二個區域網路不可具有相同的網路位址。




**在總部辦公室內路由器 A 的設定:**

1. 開啓 **VPN 與遠端存取設定**群中並選擇**遠端存取控制**，啓用必須的 VPN 服務並按下**確定**。
2. 接著，使用 PPP 爲主的服務，像是 PPTP、L2TP 等，您必須在 **PPP 基本設定**調整設定值。

VPN and Remote Access >> PPP General Setup

PPP General Setup

| PPP/MP Protocol | | IP Address Assignment for Dial-In Users (When DHCP Disable set) | |
|---|---|---|---|
| Dial-In PPP Authentication | PAP or CHAP | Start IP Address | 192.168.1.200 |
| Dial-In PPP Encryption (MPPE) | Optional MPPE | | |
| Mutual Authentication (PAP) | ○ Yes ◉ No | | |
| Username | | | |
| Password | | | |

OK

針對使用 IPSec 爲主的服務，像是 IPSec 或是以 IPSec 原則爲主的 L2TP，您必須在 **VPN IKE/ IPSec 基本設定**調整設定值，諸如雙方皆須知曉的預先共用金鑰。

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Pre-Shared Key ●●●●●

Confirm Pre-Shared Key ●●●●●

IPSec Security Method

☑ Medium (AH)

Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

OK Cancel

3. 至 **LAN-to-LAN 設定檔案**，選擇索引號碼以便編輯檔案。
4. 將一般設定如下調整，您應該啓動 VPN 連線，因爲任何一方都可啓動 VPN 連線。

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

| Profile Name | Branch1 | Call Direction | ◉ Both ○ Dial-Out ○ Dial-In |
|---|---|---|---|
| ☐ Enable this profile | | ☐ Always on | |
| Netbios Naming Packet | ◉ Pass ○ Block | Idle Timeout | 300 second(s) |
| | | ☐ Enable PING to keep alive | |
| | | PING to the IP | |

5. **撥出設定**按下圖所示調整，以便使用選定的**撥出設定**方式主動撥號連接路由器 B。如果選擇的服務項目是 ***IPSec***，您可以爲此撥號連線進一步指定遠端相對的 IP 位址、IKE 認證方式和 IPSec 安全防護方式。

**2. Dial-Out Settings**

| Type of Server I am calling | |
|---|---|
| ○ PPTP | Username ??? |
| ◉ IPSec Tunnel | Password |
| ○ L2TP with IPSec Policy None | PPP Authentication PAP/CHAP |
| | VJ Compression ◉ On ○ Off |
| Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) | **IKE Authentication Method** |
| 220.135.240.210 | ◉ Pre-Shared Key |
| | IKE Pre-Shared Key |
| | ○ Digital Signature(X.509) |
| | None |
| | **IPSec Security Method** |
| | ◉ Medium(AH) |
| | ○ High(ESP) DES without Authentication |
| | Advanced |
| | Index(1-15) in Schedule Setup: |

如果選擇的服務項目是 ***PPTP***，您可以為此撥號連線進一步指定相對 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

**2. Dial-Out Settings**

| Type of Server I am calling | |
|---|---|
| ◉ PPTP | Username draytek |
| ○ IPSec Tunnel | Password ●●●●●●● |
| ○ L2TP with IPSec Policy None | PPP Authentication PAP/CHAP |
| | VJ Compression ◉ On ○ Off |
| Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) | **IKE Authentication Method** |
| 220.135.240.210 | ◉ Pre-Shared Key |
| | IKE Pre-Shared Key |
| | ○ Digital Signature(X.509) |
| | None |
| | **IPSec Security Method** |
| | ◉ Medium(AH) |
| | ○ High(ESP) DES without Authentication |
| | Advanced |
| | Index(1-15) in Schedule Setup: |

6. 將**撥入設定**按下圖所示調整以便路由器 B 建立 VPN 連線。

如果選擇的服務項目是 ***IPSec***，您可以為此撥號連線進一步指定遠端相對的 IP 位址、認證方式和 IPSec 安全防護方式，否則系統將自動為您採用上述 **IPSec 一般設定**頁面所定義的設定。

**3. Dial-In Settings**

| Allowed Dial-In Type | |
|---|---|
| ☐ PPTP | Username: ??? |
| ☑ IPSec Tunnel | Password: |
| ☐ L2TP with IPSec Policy: None | VJ Compression: ◉ On ○ Off |
| ☑ Specify Remote VPN Gateway | **IKE Authentication Method** |
| Peer VPN Server IP: 220.135.240.210 | ☑ Pre-Shared Key |
| or Peer ID: | IKE Pre-Shared Key |
| | ☐ Digital Signature(X.509) None |
| | **IPSec Security Method** |
| | ☑ Medium(AH) |
| | High(ESP) ☑ DES ☑ 3DES ☑ AES |

如果選擇的服務項目是 ***PPTP***，您可以爲此撥號連線進一步指定相對 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

**3. Dial-In Settings**

| Allowed Dial-In Type | |
|---|---|
| ☑ PPTP | Username: draytek |
| ☐ IPSec Tunnel | Password: •••••••• |
| ☐ L2TP with IPSec Policy: None | VJ Compression: ◉ On ○ Off |
| ☑ Specify Remote VPN Gateway | **IKE Authentication Method** |
| Peer VPN Server IP: 220.135.240.210 | ☑ Pre-Shared Key |
| or Peer ID: | IKE Pre-Shared Key |
| | ☐ Digital Signature(X.509) None |
| | **IPSec Security Method** |
| | ☑ Medium(AH) |
| | High(ESP) ☑ DES ☑ 3DES ☑ AES |

7. 最後在 **TCP/IP 網路設定**欄位中設定遠端網路 IP/子網路，如此一來，路由器 A 可以透過 VPN 連線直接將封包導引至路由器 B 之遠端網路上。

**4. TCP/IP Network Settings**

| | | |
|---|---|---|
| My WAN IP | 0.0.0.0 | RIP Direction: Disable |
| Remote Gateway IP | 0.0.0.0 | From first subnet to remote network, you have to do |
| Remote Network IP | 192.168.2.0 | Route |
| Remote Network Mask | 255.255.255.0 | |
| | More | ☐ Change default route to this VPN tunnel ( Only single WAN supports this ) |

OK Clear Cancel

**在遠端辦公室內路由器 B 的設定:**

1. 開啓 **VPN 與遠端存取設定**群中並選擇**遠端存取控制**，啓用必須的 VPN 服務並按下**確定**。

2. 接著，使用 PPP 為主的服務，像是 PPTP、L2TP 等，您必須在 **PPP 一般設定** 調整設定值。

VPN and Remote Access >> PPP General Setup

PPP General Setup

| PPP/MP Protocol | | IP Address Assignment for Dial-In Users (When DHCP Disable set) | |
|---|---|---|---|
| Dial-In PPP Authentication | PAP or CHAP | Start IP Address | 192.168.2.200 |
| Dial-In PPP Encryption (MPPE) | Optional MPPE | | |
| Mutual Authentication (PAP) | ○ Yes ⦿ No | | |
| Username | | | |
| Password | | | |

OK

針對使用 IPSec 為主的服務，像是 IPSec 或是以 IPSec 政策為主的 L2TP，您必須在 **VPN IKE/ IPSec 基本設定**調整設定值，諸如雙方皆須知曉的預先共用金鑰。

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Pre-Shared Key ●●●●●

Confirm Pre-Shared Key ●●●●●

IPSec Security Method

☑ Medium (AH)

Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

OK Cancel

3. 至 **LAN-to-LAN 設定檔案**，選擇索引號碼以便編輯檔案。

4. 將**一般設定**如下調整，您應該啟動 VPN 連線，因為任何一方都可啟動 VPN 連線。

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

| | | | |
|---|---|---|---|
| Profile Name | Branch1 | Call Direction | ⦿ Both ○ Dial-Out ○ Dial-In |
| ☐ Enable this profile | | ☐ Always on | |
| Netbios Naming Packet | ⦿ Pass ○ Block | Idle Timeout | 300 second(s) |
| | | ☐ Enable PING to keep alive | |
| | | PING to the IP | |

5. **撥出設定**按下圖所示調整，以便使用選定的**撥出設定**方式主動撥號連接路由器 B。

如果選擇的服務項目是 ***IPSec***，您可以為此撥號連線進一步指定遠端相對的 IP 位址、IKE 認證方式和 IPSec 安全防護方式。

2. Dial-Out Settings

Type of Server I am calling

PPTP
IPSec Tunnel
L2TP with IPSec Policy None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
220.135.240.208

Username ???
Password
PPP Authentication PAP/CHAP
VJ Compression On Off

IKE Authentication Method
Pre-Shared Key
IKE Pre-Shared Key
Digital Signature(X.509)
None

IPSec Security Method
Medium(AH)
High(ESP) DES without Authentication
Advanced

Index(1-15) in Schedule Setup:

如果選擇的服務項目是 ***PPTP***，您可以爲此撥號連線進一步指定對方 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

2. Dial-Out Settings

Type of Server I am calling

PPTP
IPSec Tunnel
L2TP with IPSec Policy None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
220.135.240.208

Username draytek
Password ●●●●●●●
PPP Authentication PAP/CHAP
VJ Compression On Off

IKE Authentication Method
Pre-Shared Key
IKE Pre-Shared Key
Digital Signature(X.509)
None

IPSec Security Method
Medium(AH)
High(ESP) DES without Authentication
Advanced

Index(1-15) in Schedule Setup:

6. 將**撥入設定**按下圖所示調整以便路由器 A 建立 VPN 連線。

   如果選擇的服務項目是 ***IPSec***，您可以爲此撥號連線進一步指定遠端相對的 IP 位址、認證方式和 IPSec 安全防護方式，否則系統將自動爲您採用上述 **IPSec 基本設定**頁面所定義的設定。

**3. Dial-In Settings**

| Allowed Dial-In Type | |
|---|---|
| ☐ PPTP<br>☑ IPSec Tunnel<br>☐ L2TP with IPSec Policy [None] | Username [???]<br>Password [ ]<br>VJ Compression ◉ On ○ Off |
| ☑ Specify Remote VPN Gateway<br>Peer VPN Server IP<br>[220.135.240.208]<br>or Peer ID [ ] | **IKE Authentication Method**<br>☑ Pre-Shared Key<br>[IKE Pre-Shared Key] [ ]<br>☐ Digital Signature(X.509)<br>[None]<br>**IPSec Security Method**<br>☑ Medium(AH)<br>High(ESP) ☑ DES ☑ 3DES ☑ AES |

如果選擇的服務項目是 ***PPTP***，您可以爲此撥號連線進一步指定相對 IP 位址、使用者名稱、密碼和 VJ 壓縮等。

**3. Dial-In Settings**

| Allowed Dial-In Type | |
|---|---|
| ☑ PPTP<br>☐ IPSec Tunnel<br>☐ L2TP with IPSec Policy [None] | Username [draytek]<br>Password [●●●●●●●]<br>VJ Compression ◉ On ○ Off |
| ☑ Specify Remote VPN Gateway<br>Peer VPN Server IP<br>[220.135.240.208]<br>or Peer ID [ ] | **IKE Authentication Method**<br>☑ Pre-Shared Key<br>[IKE Pre-Shared Key] [ ]<br>☐ Digital Signature(X.509)<br>[None]<br>**IPSec Security Method**<br>☑ Medium(AH)<br>High(ESP) ☑ DES ☑ 3DES ☑ AES |

7. 最後在 **TCP/IP Network Settings** 設定遠端網路 IP/子網路，如此一來，路由器 B 可以透過 VPN 連線直接將封包導引至路由器 A 之遠端網路上。

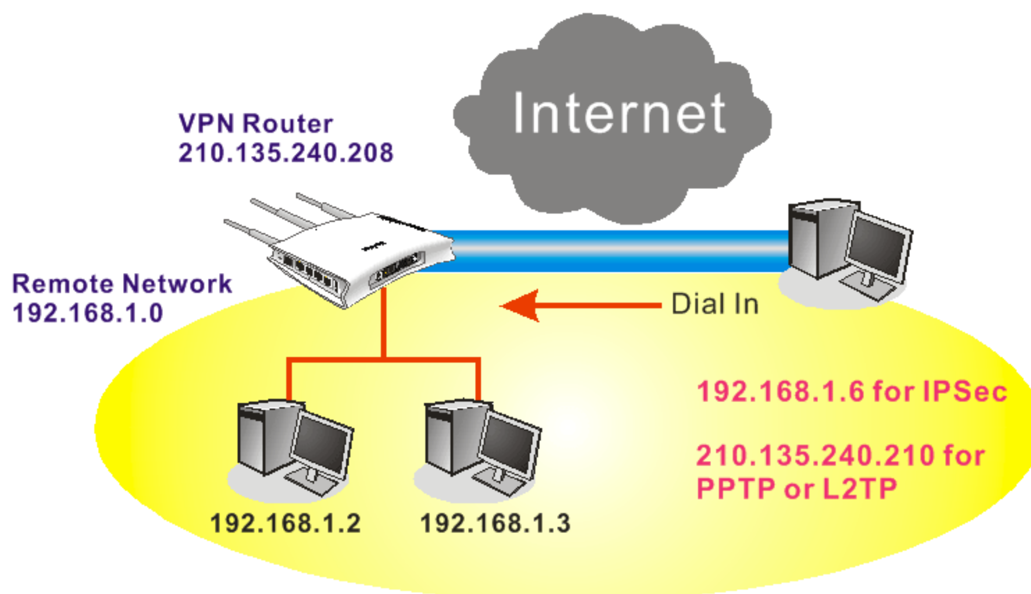
**4. TCP/IP Network Settings**

| | | |
|---|---|---|
| My WAN IP | 0.0.0.0 | RIP Direction [Disable] |
| Remote Gateway IP | 0.0.0.0 | From first subnet to remote network, you have to do |
| Remote Network IP | 192.168.1.0 | [Route] |
| Remote Network Mask | 255.255.255.0 | |
| | [More] | ☐ Change default route to this VPN tunnel ( Only single WAN supports this ) |

[OK] [Clear] [Cancel]

## 5.2 建立工作者和總部之間的 VPN 遠端撥號連線

另一個常用的範例是：作爲一個工作者，您可能想要安全地連接到企業網路，依照下面所顯示的網路結構，您可以遵照相關的步驟來建立遠端用戶設定檔，並且在遠端主機上安裝 Smart VPN Client。




**在辦公室內VPN路由器的設定:**

1. 開啓 **VPN 與遠端存取設定**群中並選擇**遠端存取控制**，啓用必須的 VPN 服務並按下**確定**。
2. 接著，使用 PPP 爲主的服務，像是 PPTP、L2TP 等，您必須在 **PPP 基本設定**調整設定值。

VPN and Remote Access >> PPP General Setup

PPP General Setup

| PPP/MP Protocol | | IP Address Assignment for Dial-In Users (When DHCP Disable set) | |
|---|---|---|---|
| Dial-In PPP Authentication | PAP or CHAP | Start IP Address | 192.168.1.200 |
| Dial-In PPP Encryption (MPPE) | Optional MPPE | | |
| Mutual Authentication (PAP) | ○ Yes ◉ No | | |
| Username | | | |
| Password | | | |

OK

如果選擇的服務項目是 ***IPSec***，如 IPsec 或是 IPSec 原則之 L2TP，您必須設定 **IKE/IPSec 基本設定**像是雙方都應知曉的預設共用金鑰。

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Pre-Shared Key ●●●●●

Confirm Pre-Shared Key ●●●●●

IPSec Security Method

☑ Medium (AH)

Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

OK Cancel

3. 至**遠端撥入使用者**，按任一索引編號以編輯設定檔。
4. 將**撥入設定**按下圖所示調整，以便遠端使用者建立 VPN 連線。

如果選擇的服務項目是 ***IPSec***，您可以為此撥號連線進一步指定遠端相對的 IP 位址、IKE 認證方式和 IPSec 安全防護方式，否則系統將自動為您採用上述 **IPSec 基本設定**頁面所定義的設定。

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication

☐ Enable this account

Idle Timeout 300 second(s)

Allowed Dial-In Type

☐ PPTP

☑ IPSec Tunnel

☐ L2TP with IPSec Policy None

☐ Specify Remote Node

Remote Client IP or Peer ISDN Number

or Peer ID

Netbios Naming Packet ◉ Pass ○ Block

Username ???

Password

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key

☐ Digital Signature(X.509)

None

IPSec Security Method

☑ Medium(AH)

High(ESP) ☑ DES ☑ 3DES ☑ AES

Local ID (optional)

OK Clear Cancel

如果選擇的服務項目是 ***PPTP***，您應該為此撥號連線進一步指定遠端相對的 IP 位址、使用者名稱、密碼以及 VJ 壓縮。

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication
Enable this account
Idle Timeout 300 second(s)

Allowed Dial-In Type
PPTP
IPSec Tunnel
L2TP with IPSec Policy None

Specify Remote Node
Remote Client IP or Peer ISDN Number

or Peer ID

Netbios Naming Packet Pass Block

Username ???
Password

IKE Authentication Method
Pre-Shared Key
IKE Pre-Shared Key
Digital Signature(X.509)
None

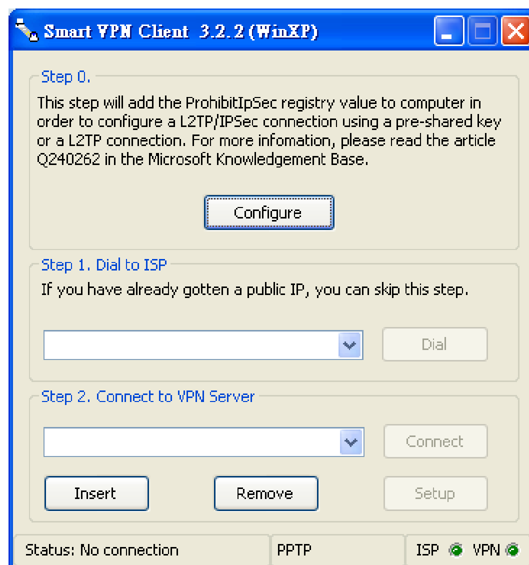
IPSec Security Method
Medium(AH)
High(ESP) DES 3DES AES
Local ID (optional)

OK Clear Cancel

**遠端主機上的設定:**

1. 對 Win98/ME 系統而言，您可以使用 Dial-up Networking 建立 PPTP 通道給予路由器；對 Win2000/XP 來說，請使用 Network and Dial-up connections 或是 Smart VPN Client 等軟體幫忙建立 PPTP、L2TP 和 L2TP over IPSec 通道，您可以在包裝的光碟片中找到此軟體或是進入 http://www.draytek.com/ 網站下載中心取得，依照螢幕指示來安裝即可。

2. 在安裝成功之後，對於第一次使用的用戶，必須先按 **Step 0** 中的 **Configure** 按鈕，重新啓動主機。




3. 在 **Step 2. Connect to VPN Server** 中，按下 **Insert** 按鈕新增一個新的入口。

如果選擇的服務項目是 ***IPSec Tunnel***，如下圖所示：

Dial To VPN

Session Name: Office

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

192.168.1.1

User Name : draytek_user1

Password : ********

Type of VPN

PPTP L2TP

IPSec Tunnel L2TP over IPSec

PPTP Encryption

No encryption

Require encryption

Maximum strength encryption

Use default gateway on remote network

OK Cancel

您可以進一步指定取得 IP、安全防護以及驗證的方法。若已選擇 Pre-Shared Key，那麼此設定必須與 VPN 路由器中的設定一致。

IPSec Policy Setting

My IP : 172.16.3.100

Type of IPSec

Standard IPSec Tunnel

Remote Subnet : 0 . 0 . 0 . 0

Remote Subnet Mask : 255 . 255 . 255 . 0

Virture IP DrayTek Virture Interface

Obtain an IP address automatically (DHCP over IPSec)

Specify an IP address

IP Address: 192 . 168 . 1 . 201

Subnet Mask: 255 . 255 . 255 . 0

Security Method

Medium(AH) High(ESP)

MD5 DES

Authority Method

Pre-shared Key : ******

Certification Authority:

Browse...

OK Cancel

如果選擇的服務項目是 ***PPTP***，您可以進一步指定 VPN 伺服器 IP 位址、使用者名稱、密碼和加密方法，使用者名稱和密碼必須和您在 VPN 路由器中所設定的內容一致。如欲使用遠端網路上預設的閘道，表示所有遠端主機上的封包都將會導引至 VPN 伺服器，然後再轉送到網際網路上，這樣會讓遠端主機看起來像是在企業網路上運作一般。

Dial To VPN

Session Name: office

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

192.168.1.1

User Name : draytek_user1

Password : *****

Type of VPN

PPTP L2TP

IPSec Tunnel L2TP over IPSec

PPTP Encryption

No encryption

Require encryption

Maximum strength encryption

Use default gateway on remote network

OK Cancel

4. 按 **Connect** 按鈕建立連線，當連線成功之時，您可以在右下方角落發現到綠色閃燈。

## 5.3 QoS 設定範例

假定電信工作人員有時在家中工作並且需要照料小孩，在工作時間，工作人員可使用家中的路由器，透過 HTTPS 或是 VPN 連接上總部的伺服器，來檢查電子郵件並存取公司內部的資料庫訊息，同時，小朋友也可以在休息室透過 VoIP 或是 Skype 彼此交談。

1. 進入**頻寬管理**之**服務品質**頁面。

Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

| Status | Bandwidth | Directon | Class 1 | Class 2 | Class 3 | Others | UDP Bandwidth Control | |
|---|---|---|---|---|---|---|---|---|
| Enable | 10000Kbps/10000Kbps | Outbound | 25% | 25% | 25% | 25% | Inactive | Setup |

Class Rule

| Index | Name | Rule | Service Type |
|---|---|---|---|
| Class 1 | Test | Edit | |
| Class 2 | | Edit | Edit |
| Class 3 | | Edit | |

2. 按WAN1 的**設定**連結開啓頁面，請確定左上角的**啓用服務品質(QoS)控制功能**已經勾選，選擇**雙向**作爲方向。

Bandwidth Management >> Quality of Service

General Setup

☑ Enable the QoS Control [OUT] (IN / OUT / BOTH)

WAN Inbound Bandwidth

WAN Outbound Bandwidth

3. 回至上一層，按類別 1 的**編輯**連結以輸入索引類別 1 的名稱 “**E-mail**”，再按**確定**。

Bandwidth Management >> Quality of Service

Class Index #1

Name: E-mail

| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
|---|---|---|---|---|---|
| 1 ○ | Active | Any | Any | IP precedence 2 | TFTP(UDP:69) |

Add  Edit  Delete

OK  Cancel

4. 使用者可設定保留頻寬(例如 25%) 給予透過POP3 和SMTP通訊協定來傳送的電子郵件。參考下圖。

Bandwidth Management >> Quality of Service

General Setup

☑ Enable the QoS Control [BOTH]

WAN Inbound Bandwidth 10000 Kbps

WAN Outbound Bandwidth 10000 Kbps

| Index | Class Name | Reserved_bandwidth Ratio |
|---|---|---|
| Class 1 | E-mail | 25 % |
| Class 2 | | 25 % |
| Class 3 | | 25 % |
| | Others | 25 % |

☐ Enable UDP Bandwidth Control — Limited_bandwidth Ratio 25 %

☐ Outbound TCP ACK Prioritize — Online Statistics

OK  Clear  Cancel

5. 回至上一層，按類別 2 的**編輯**連結以輸入索引類別 2 的名稱” **HTTP**”，再按**確定**。於此索引中我們可以設定保留頻寬(例如 25%)給予**HTTP**。

Bandwidth Management >> Quality of Service

Class Index #2

Name HTTPS

| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
|---|---|---|---|---|---|
| 1 | Active | Any | Any | ANY | TFTP(UDP:69) |

Add Edit Delete

OK Cancel

6. 選擇WAN的**設定**連結。

Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

| Status | Bandwidth | Directon | Class 1 | Class 2 | Class 3 | Others | UDP Bandwidth Control | |
|---|---|---|---|---|---|---|---|---|
| Enable | 10000Kbps/10000Kbps | Both | 25% | 25% | 25% | 25% | Inactive | Setup |

Class Rule

| Index | Name | Rule | Service Type |
|---|---|---|---|
| Class 1 | E-mail | Edit | Edit |
| Class 2 | HTTPS | Edit | |
| Class 3 | | Edit | |

7. 勾選**啓用UDP頻寬控制**防止VoIP大量的UDP資料影響其他的應用程式。

Bandwidth Management >> Quality of Service

General Setup

☑ Enable the QoS Control BOTH

WAN Inbound Bandwidth 10000 Kbps

WAN Outbound Bandwidth 10000 Kbps

| Index | Class Name | Reserved_bandwidth Ratio |
|---|---|---|
| Class 1 | E-mail | 25 % |
| Class 2 | HTTPS | 25 % |
| Class 3 | | 25 % |
| | Others | 25 % |

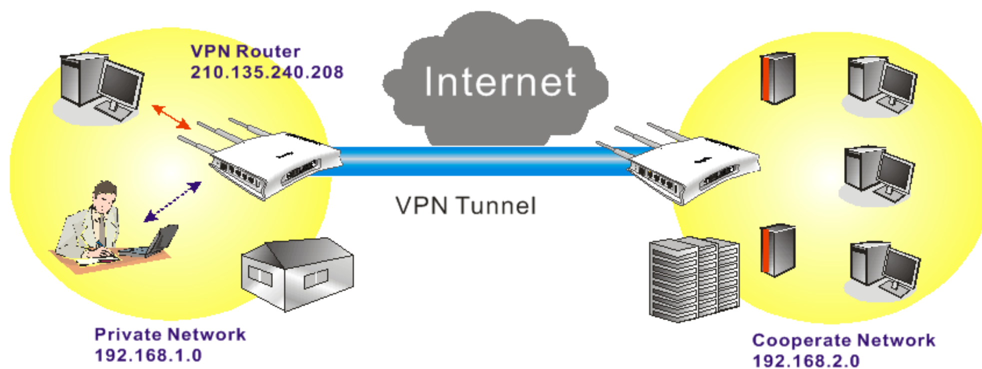
☑ Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 %

☐ Outbound TCP ACK Prioritize Online Statistics

OK Clear Cancel

8. 如果工作人員利用主機對主機的VPN通道，連上了總公司，(詳細設定請參考VPN一節)他可能已設定了相關的索引內容，請輸入索引編號 3 的類別名稱，在此類別

中，工作人員將可完成一條VPN通道的保留頻寬設定。




Bandwidth Management >> Quality of Service

Class Index #3

Name VPN

| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
|---|---|---|---|---|---|
| 1 | Empty | - | - | - | - |

Add Edit Delete

OK Cancel

9. 按**編輯**開啓下述視窗，勾選**ACT** 方塊。.

Bandwidth Management >> Quality of Service

Rule Edit

☑ ACT

Local Address Any Edit

Remote Address Any Edit

DiffServ CodePoint IP precedence 2

Service Type SYSLOG(UDP:514)

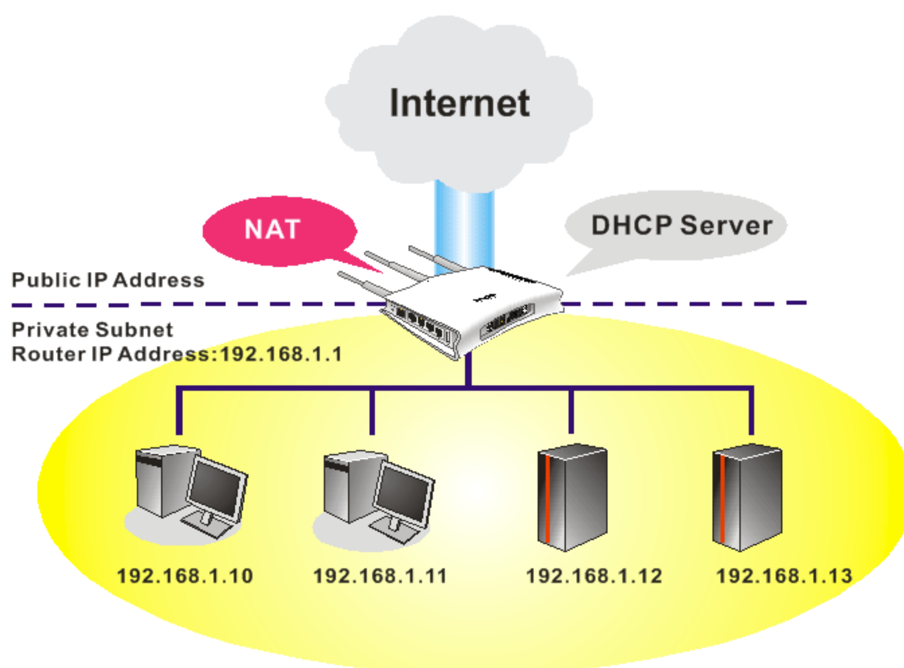
Note: Please choose/setup the Service Type first.

OK Cancel

10. 然後按**本地位址**中的**編輯**按鈕，設定工作人員的子網位址，再按下**遠端位址**的**編輯**按鈕設定總公司的IP位址，最後按此網頁的**確定**按鈕。

## 5.4 使用 NAT 來建立區域連線

預設設定和相關應用範例顯示如下，預設路由器之虛擬 IP 位址/子網路遮罩爲 192.168.1.1/255.255.255.0，內建之 DHCP 伺服器已經啓用，因此指定每個已 NAT 的主機一個 192.168.1.x 的 IP 位址，範圍從 192.168.1.10 開始。




只有紅色框內的設定需要調整，以符合 NAT 用途的需求。

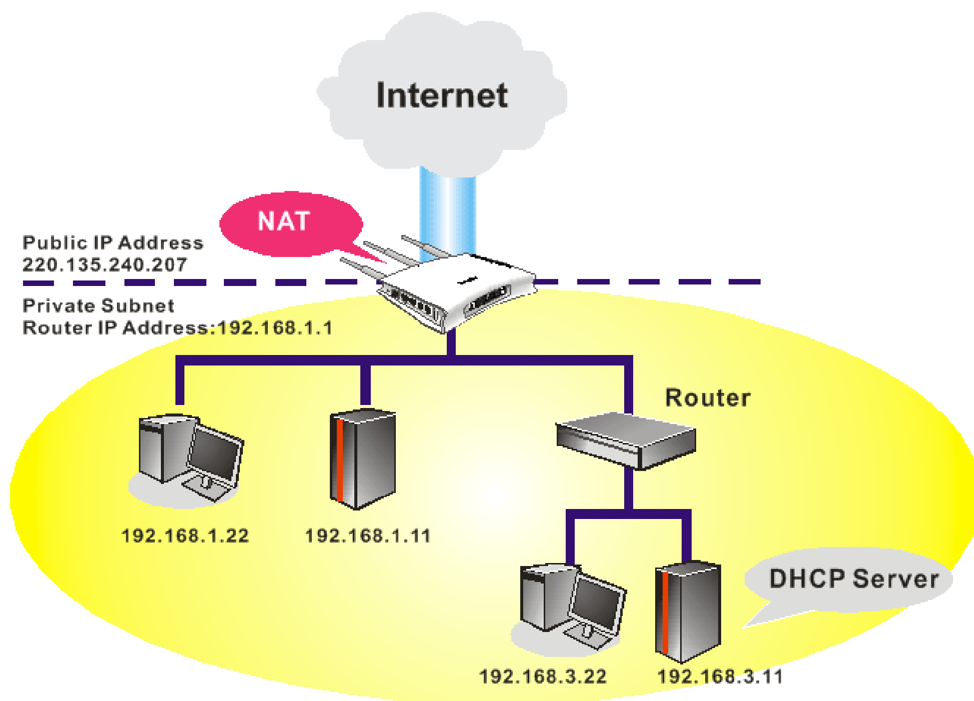
**LAN >> General Setup**

**Ethernet TCP / IP and DHCP Setup**

| LAN IP Network Configuration | | DHCP Server Configuration | |
|---|---|---|---|
| For NAT Usage | | ◉ Enable Server ○ Disable Server | |
| 1st IP Address | 192.168.1.5 | Relay Agent: ○ 1st Subnet ○ 2nd Subnet | |
| 1st Subnet Mask | 255.255.255.0 | Start IP Address | 192.168.1.10 |
| For IP Routing Usage ○ Enable ◉ Disable | | IP Pool Counts | 50 |
| 2nd IP Address | 192.168.2.1 | Gateway IP Address | 192.168.1.5 |
| 2nd Subnet Mask | 255.255.255.0 | DHCP Server IP Address for Relay Agent | |
| | 2nd Subnet DHCP Server | **DNS Server IP Address** | |
| RIP Protocol Control | Disable | ☐ Force DNS manual setting | |
| | | Primary IP Address | |
| | | Secondary IP Address | |

OK

如要使用網路中的 DHCP 伺服器而非路由器內建的伺服器，您必須變更設定，如下所示：




只有紅色框內的設定需要調整，以符合 NAT 用途的需求。

**LAN >> General Setup**

**Ethernet TCP / IP and DHCP Setup**

| LAN IP Network Configuration | | DHCP Server Configuration | |
|---|---|---|---|
| For NAT Usage | | ○ Enable Server ◉ Disable Server | |
| 1st IP Address | 192.168.1.5 | Relay Agent: ○ 1st Subnet ○ 2nd Subnet | |
| 1st Subnet Mask | 255.255.255.0 | Start IP Address | 192.168.1.10 |
| For IP Routing Usage ○ Enable ◉ Disable | | IP Pool Counts | 50 |
| 2nd IP Address | 192.168.2.1 | Gateway IP Address | 192.168.1.5 |
| 2nd Subnet Mask | 255.255.255.0 | DHCP Server IP Address for Relay Agent | 192.168.3.11 |
| | 2nd Subnet DHCP Server | **DNS Server IP Address** | |
| RIP Protocol Control | Disable | ☐ Force DNS manual setting | |
| | | Primary IP Address | |
| | | Secondary IP Address | |

OK

# 5.5 VoIP 功能使用範例

## 5.5.1 透過 SIP 伺服器撥打電話

### 範例 1: John 和 David 有來自不同服務供應商提供的 SIP 位址

John 的 SIP URL: 1234@draytel.org, David 的 SIP URL: 4321@iptel.org

**John 端的設定**

電話簿索引號碼 1
電話號碼: 1111
顯示名稱: David
SIP URL: 4321@iptel.org

**SIP 帳號設定---**

設定檔名稱: draytel1
由此註冊: 自動
SIP 通訊埠: 5060 (預設值)
網域: draytel.org
伺服器: draytel.org
以對外伺服器之身分運作: 不勾選
顯示名稱: John
帳號名稱/號碼: 1234
驗證 ID 身分: 不勾選密碼: ****
有效時間: (使用預設值)

**CODEC/RTP/DTMF ---**
(使用預設值)

VoIP >> DialPlan Setup

Phone Book Index No. 1

☑ Enable

| | |
|---|---|
| Phone Number | 1111 |
| Display Name | David |
| SIP URL | 4321 @ iptel.org |
| Dial Out Account | Default |
| Loop through | None |
| Backup Phone Number | |

OK Clear Cancel

VoIP >> SIP Accounts

SIP Account Index No. 1

| | |
|---|---|
| Profile Name | draytel 1 (11 char max.) |
| Register | Auto ☐ Call without Registration |
| SIP Port | 5060 |
| Domain/Realm | draytel.org (63 char max.) |
| Proxy | draytel.org (63 char max.) |
| ☐ Act as outbound proxy | |
| Display Name | John (23 char max.) |
| Account Number/Name | 1234 (63 char max.) |
| ☐ Authentication ID | (63 char max.) |
| Password | •••• (63 char max.) |
| Expiry Time | 1 hour 3600 sec |
| NAT Traversal Support | None |
| Ring Port | ☑ Phone 1 ☐ Phone 2 |
| Ring Pattern | 1 |

OK Cancel

**John 打電話給 David ---**
拿起電話撥打 1111# (David 的電話號碼)

**David 端的設定**

DialPlan 索引號碼 1
電話號碼:2222
顯示名稱: John
SIP URL:1234@draytel.org

**SIP 帳號設定 ---**

設定檔名稱: iptel 1
由此註冊: 自動
SIP 通訊埠: 5060(預設值)
網域: iptel.org
伺服器: iptel.org
以對外伺服器之身分運作: 不勾選
顯示名稱: David
帳號名稱/號碼: 4321
驗證 ID 身分: 不勾選
密碼: ****
有效時間: (使用預設值)

**CODEC/RTP/DTMF ---**

VoIP >> DialPlan Setup

Phone Book Index No. 1

☑ Enable

| | |
|---|---|
| Phone Number | 2222 |
| Display Name | John |
| SIP URL | 1234 @ draytel.org |
| Dial Out Account | Default |
| Loop through | None |
| Backup Phone Number | |

OK Clear Cancel

VoIP >> SIP Accounts

SIP Account Index No. 1

| | |
|---|---|
| Profile Name | iptel 1 (11 char max.) |
| Register | Auto ☐ Call without Registration |
| SIP Port | 5060 |
| Domain/Realm | iptel.org (63 char max.) |
| Proxy | iptel.org (63 char max.) |
| ☐ Act as outbound proxy | |
| Display Name | David (23 char max.) |
| Account Number/Name | 4321 (63 char max.) |
| ☐ Authentication ID | (63 char max.) |
| Password | •••• (63 char max.) |
| Expiry Time | 1 hour 3600 sec |
| NAT Traversal Support | None |
| Ring Port | ☑ Phone 1 ☐ Phone 2 |
| Ring Pattern | 1 |

OK Cancel

**David 打電話給 John**
拿起電話撥打 2222# (John 的電話號碼)

(使用預設值)

**範例 2: John 和 David 都有來自相同服務供應商提供的 SIP 位址**

John 的 SIP URL: 1234@draytel.org , David 的 SIP URL: 4321@draytel.org

**John 端的設定**

DialPlan 索引|號碼 1
電話號碼: 1111
顯示名稱: David
SIP URL: 4321@draytel.org

**SIP 帳號設定 ---**

設定檔名稱: draytel 1
由此註冊: 自動
SIP 通訊埠: 5060 (預設值)
網域: draytel.org
伺服器: draytel.org
以對外伺服器之身分運作: 不勾選
顯示名稱: John
帳號名稱/號碼: 1234
驗證 ID 身分: 不勾選
密碼: ****
有效時間: (使用預設值)

**CODEC/RTP/DTMF ---**
(Use default value)

VoIP >> DialPlan Setup

Phone Book Index No. 1
☑ Enable
Phone Number: 1111
Display Name: David
SIP URL: 4321 @ draytel.org
Dial Out Account: Default
Loop through: None
Backup Phone Number:
OK | Clear | Cancel

VoIP >> SIP Accounts

SIP Account Index No. 1
Profile Name: draytel 1 (11 char max.)
Register: Auto ☐ Call without Registration
SIP Port: 5060
Domain/Realm: draytel.org (63 char max.)
Proxy: draytel.org (63 char max.)
☐ Act as outbound proxy
Display Name: John (23 char max.)
Account Number/Name: 1234 (63 char max.)
☐ Authentication ID (63 char max.)
Password: •••• (63 char max.)
Expiry Time: 1 hour 3600 sec
NAT Traversal Support: None
Ring Port: ☑ Phone 1 ☐ Phone 2
Ring Pattern: 1
OK | Cancel

**John 打電話給 David**

拿起電話撥打 1111# (David 的電話簿號碼) 或,
拿起電話撥打 4321# (David 的帳號名稱)

**David 端的設定**

DialPlan 索引|號碼 1
電話號碼:2222
顯示名稱: John
SIP URL:1234@draytel.org

**SIP 帳號設定---**

設定檔名稱: John
由此註冊:自動
SIP 通訊埠: 5060(預設值)
網域: draytel.org
伺服器: draytel.org
以對外伺服器之身分運作: 不勾選
顯示名稱: David
帳號名稱/號碼: 4321
驗證 ID 身分: 不勾選
密碼: ****
有效時間: (使用預設值)

**CODEC/RTP/DTMF---**
(使用預設值)

VoIP >> DialPlan Setup

Phone Book Index No. 1
☑ Enable
Phone Number: 2222
Display Name: John
SIP URL: 1234 @ draytel.org
Dial Out Account: Default
Loop through: None
Backup Phone Number:
OK | Clear | Cancel

VoIP >> SIP Accounts

SIP Account Index No. 1
Profile Name: draytel 1 (11 char max.)
Register: Auto ☐ Call without Registration
SIP Port: 5060
Domain/Realm: draytel.org (63 char max.)
Proxy: draytel.org (63 char max.)
☐ Act as outbound proxy
Display Name: David (23 char max.)
Account Number/Name: 4321 (63 char max.)
☐ Authentication ID (63 char max.)
Password: •••• (63 char max.)
Expiry Time: 1 hour 3600 sec
NAT Traversal Support: None
Ring Port: ☑ Phone 1 ☐ Phone 2
Ring Pattern: 1
OK | Cancel

**David 打電話給 John**

拿起電話撥打 2222# (John 的電話簿號碼) 或
拿起電話撥打 1234# (John 的帳號名稱)

## 5.5.2 點對點撥打電話

**範例 2:** Arnor 和 Paulin 分別擁有路由器，雙方可以不經過 SIP 註冊而撥打電話給彼此，首先他們必須具有雙方的 IP 位址，並指定用來撥號的帳號名稱。

Arnor 的 SIP URL: 1234@214.61.172.53　Paulin 的 SIP URL: 4321@ 203.69.175.24

**Arnor 端的設定**

DialPlan 索引號碼 1
電話號碼: 1111
顯示名稱: paulin
SIP URL: 4321@ 203.69.175.24

VoIP >> DialPlan Setup

Phone Book Index No. 1

| | |
|---|---|
| ☑ Enable | |
| Phone Number | 1111 |
| Display Name | paulin |
| SIP URL | 4321 @ 203.69.175.24 |
| Dial Out Account | Default |
| Loop through | None |
| Backup Phone Number | |

OK　Clear　Cancel

**SIP 帳號設定 ---**

設定檔名稱: Paulin
由此註冊: 無
SIP 通訊埠: 5060(預設值)
網域: (空白)
伺服器: (空白)
以對外伺服器之身分運作: 不勾選顯示名稱: Arnor
帳號名稱/號碼: 1234
驗證 ID 身分: 不勾選
密碼: (空白)
有效時間: (使用預設值)

VoIP >> SIP Accounts

SIP Account Index No. 1

| | | |
|---|---|---|
| Profile Name | Paulin | (11 char max.) |
| Register | Auto | ☐ Call without Registration |
| SIP Port | 5060 | |
| Domain/Realm | | (63 char max.) |
| Proxy | | (63 char max.) |
| ☐ Act as outbound proxy | | |
| Display Name | Arnor | (23 char max.) |
| Account Number/Name | 1234 | (63 char max.) |
| ☐ Authentication ID | | (63 char max.) |
| Password | •••• | (63 char max.) |
| Expiry Time | 1 hour　3600 | sec |
| NAT Traversal Support | None | |
| Ring Port | ☑ Phone 1 ☐ Phone 2 | |
| Ring Pattern | 1 | |

OK　Cancel

**CODEC/RTP/DTMF---**

(使用預設值)

**Arnor 打電話給 Paulin**

拿起電話撥打 **1111#** (Arnor 的電話簿號碼)

**Paulin 端的設定**

DialPlan 索引號碼 1
電話號碼:2222
顯示名稱: Arnor
SIP URL: 1234@214.61.172.53

VoIP >> DialPlan Setup

Phone Book Index No. 1

| | |
|---|---|
| ☑ Enable | |
| Phone Number | 2222 |
| Display Name | Arnor |
| SIP URL | 1234 @ 214.61.172.53 |
| Dial Out Account | Default |
| Loop through | None |
| Backup Phone Number | |

OK　Clear　Cancel

**SIP 帳號設定 ---**

設定檔名稱: Arnor
由此註冊: 無
SIP 通訊埠: 5060(預設值)
網域: (空白)
伺服器: (空白)
以對外伺服器之身分運作: 不勾選顯示名稱: Paulin
帳號名稱/號碼: 4321
驗證 ID 身分: 不勾選
密碼: (空白)
有效時間: (使用預設值)

VoIP >> SIP Accounts

SIP Account Index No. 1

| | | |
|---|---|---|
| Profile Name | Arnor | (11 char max.) |
| Register | Auto | ☐ Call without Registration |
| SIP Port | 5060 | |
| Domain/Realm | | (63 char max.) |
| Proxy | | (63 char max.) |
| ☐ Act as outbound proxy | | |
| Display Name | Paulin | (23 char max.) |
| Account Number/Name | 4321 | (63 char max.) |
| ☐ Authentication ID | | (63 char max.) |
| Password | •••• | (63 char max.) |
| Expiry Time | 1 hour　3600 | sec |
| NAT Traversal Support | None | |
| Ring Port | ☑ Phone 1 ☐ Phone 2 | |
| Ring Pattern | 1 | |

OK　Cancel

**CODEC/RTP/DTMF---**

(使用預設值)

**Paulin 打電話給 Arnor**

拿起電話撥打 **2222#** (John 的電話簿號碼)

# 5.6 更新路由器韌體

更新韌體之前，您必須先安裝路由器工具，**Firmware Upgrade Utility** 即包含在 CD 中。

1. 將光碟片放進光碟槽中。
2. 請自網頁中，找出**工具程式**選單並點選進入頁面。
3. 在**工具程式**網頁上，按 **Install Now!** (位於 Syslog 說明下方) 以安裝相關程式。

Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

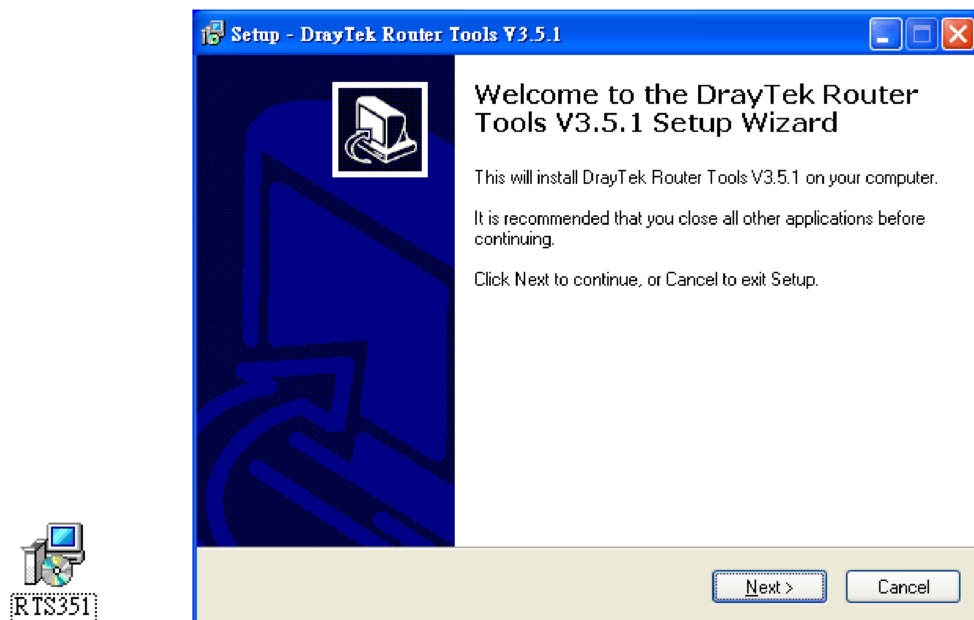



4. **RTSxxx.exe** 檔案將會複製到您的電腦上，請記住執行檔的儲存位置。
5. 進入 **www.draytek.com.tw** 網站，以尋找目前該路由器最新的韌體檔案。
6. Access into **Support Center >> Downloads**. Find out the model name of the router and click the firmware link. The Tools of Vigor router will display as shown below. 進入**支援服務 >> 檔案下載**，找到路由器機型名稱之後，選取其相關的韌體連結，**工具**畫面將出現如下：

| Tools Name | Released Date | Version | OS | Support Model | Download |
|---|---|---|---|---|---|
| Router Tools | 21/12/2006 | 3.5.1 | MS-Windows | All Model | zip |
| Smart VPN Client | 18/08/2006 | 3.2.6 | MS-Windows | All Model | zip |
| LPR | 27/06/2005 | 1.0 | MS-Windows | For Print Function | zip |
| VTA | 15/09/2005 | 2.8 | Windows2000/XP | For ISDN Model | zip |
| DialPlan | 26/01/2006 | 2.5_lite | MS-Windows | For VoIP Model | zip |

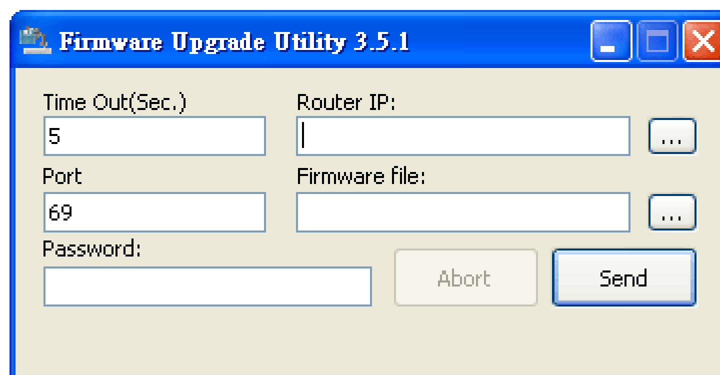
7. 插入路由器的 CD，請至相關連結處下載正確的韌體檔案(zip 檔案)。
8. 接著，解壓縮 ZIP 檔案。

9. 在路由器工具圖示上按二下，安裝精靈將出現如下：



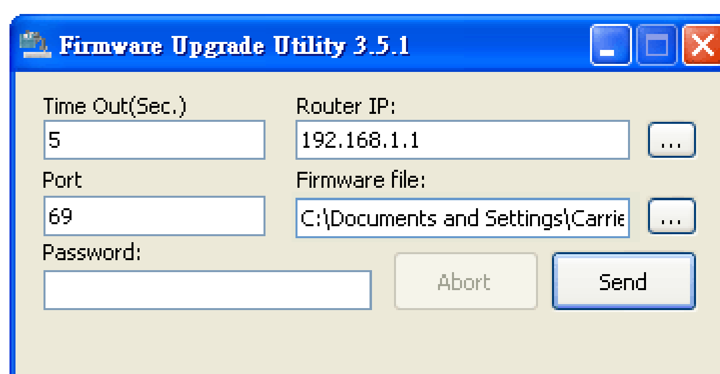

10. 依照螢幕指示安裝此工具，按下 **Finish** 以結束安裝。

11. 自**開始(Start)**選單中，指向**程式集(Programs)**，然後選擇 **Router Tools XXX >> Firmware Upgrade Utility**。

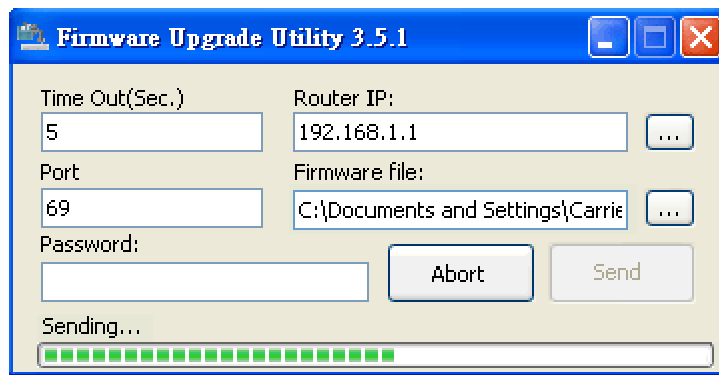



12. 輸入路由器 IP 地址，通常為 **192.168.1.1**。

13. 按韌體檔案(Firmware file)輸入欄右邊的按鈕，尋找您自公司網站下載之韌體檔案，您會看見二個副檔名不同的檔案：**xxxx.all** (可保持用戶原先的設定)以及 **xxxx.rst** (將用戶設定重新回復預設值)，請按照實際需要選擇任何一個。

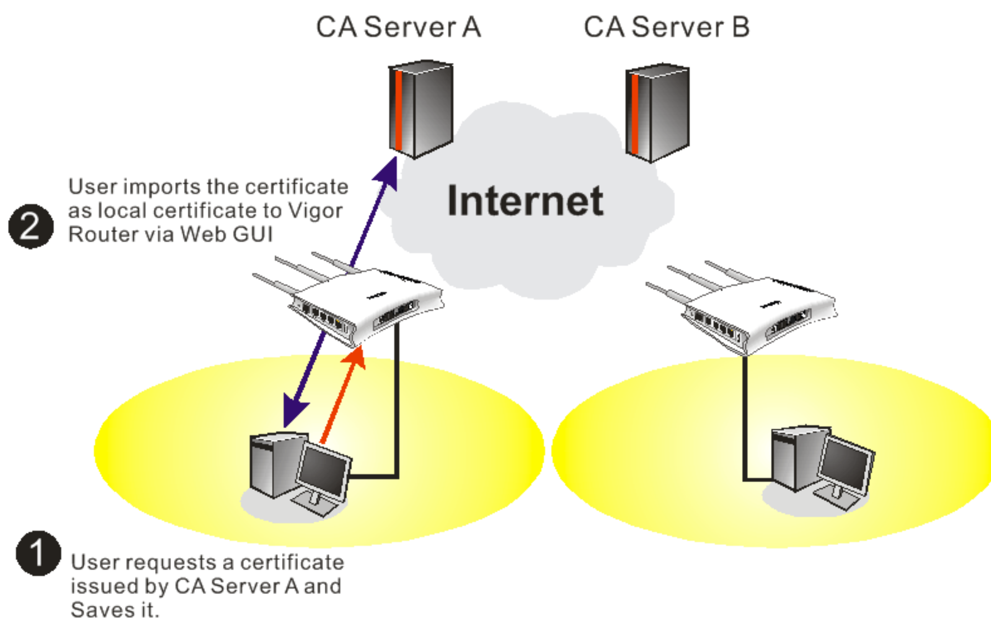


14. 按下 **Send**。




15. 現在韌體更新已完成。

## 5.7 在 Windows CA 伺服器上提出憑證需求




1. 選擇**憑證管理>>本機憑證**。

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

| Name | Subject | Status | Modify |
| --- | --- | --- | --- |
| Local | --- | --- | View Delete |

GENERATE IMPORT REFRESH

X509 Local Certificate

2. 按**產生**按鈕開始編輯憑證需求，請輸入必要的資訊。

Certificate Management >> Local Certificate

Generate Certificate Request

| Subject Alternative Name | |
|---|---|
| Type | IP Address |
| IP | |
| **Subject Name** | |
| Country (C) | |
| State (ST) | |
| Location (L) | |
| Orginization (O) | |
| Orginization Unit (OU) | |
| Common Name (CN) | |
| Email (E) | |
| **Key Type** | RSA |
| **Key Size** | 1024 Bit |

Generate

3. 複製並儲存 X509 本機憑證需求，稍後將會應用到此文字檔。

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

| Name | Subject | Status | Modify |
|---|---|---|---|
| Local | /C=TW/ST=HC/L=HC/O=Draytek/O... | Requesting | View Delete |

GENERATE IMPORT REFRESH

X509 Local Certificate


```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH
EwJIQzEQMA4GA1UEChMHRHJheXRlazELMAkGA1UECxMCUkQxIjAgBgkqhkiG9w0B
CQEWE3N1cHBvcnRAZHJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTU5HQvXpAzcrgJBGrikTUBX
a1X//fgnEccQA2LPSQIQ85Qychwq07BmOEDf10wHwCalAZQoGvIiODMC7f5w9xA8
m6+Of4xZ4QQnjXXgciCOBj1iAa6MLScelsynZhkgnQ1QN5uFAgMBAAGgADANBgkq
hkiG9w0BAQUFAAOBgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYDZefCmGfX
9yojHpstNsmWsMRuAwGeKCWc8S/gLtHhr6iccMoToQFx/LWdaEPU5LqryBKKgC9t
eorpDa1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvclhWFSXKVLU7g==
-----END CERTIFICATE REQUEST-----
```


4. 透過網頁瀏覽器連接 CA 伺服器，依照螢幕指示完成需求設定。下圖我們以 Windows 2000 CA 伺服器為範本，請選擇 **Request a Certificate**。

*Microsoft* Certificate Services -- vigor **Home**

**Welcome**

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

**Select a task:**

- ○ Retrieve the CA certificate or certificate revocation list
- ◉ Request a certificate
- ○ Check on a pending certificate

Next >

選擇 **Advanced request**，然後按 **Next**。

**Microsoft** Certificate Services -- vigor **Home**

**Choose Request Type**

Please select the type of request you would like to make:

○ User certificate request:

User Certificate

◉ Advanced request

Next >

挑選 **Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**，然後按 **Next**。

**Microsoft** Certificate Services -- vigor **Home**

**Advanced Certificate Requests**

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

○ Submit a certificate request to this CA using a form.

◉ Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
*You must have an enrollment agent certificate to submit a request for another user.*

Next >

匯入 X509 本機憑證文字檔，選擇 **Router (Offline request)** 或 **PSec (Offline request)** 。

**Microsoft** Certificate Services -- vigor **Home**

**Submit A Saved Request**

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

**Saved Request:**

Base64 Encoded Certificate Request (PKCS #10 or #7):


-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAO
BgkqhkiG9w0BCQEWEXByZXNzQGRyYX1oZWsuY29t
A4GNADCBiQKBgQDQYB7wmZFfFhN9/IeQnG03Xk++
hX4bp89cUF9d1oACGGiM/tcBOckdcZdPFFvIXcP3
x/GOA7CTvO/fQzpxroCw1JTjLSjS0/Bn9v50951G


Browse for a file to insert.

**Certificate Template:**

Administrator

Administrator
Authenticated Session
Basic EFS
EFS Recovery Agent
User
IPSEC (Offline request)
Router (Offline request)
Subordinate Certification Authority
Web Server

**Additional Attribut**

Attributes:

Submit >

需求提出後，伺服器會給您一個憑證，請選擇 **ase 64 encoded** 憑證及下載該憑證，現在您應該會從伺服器取得一個憑證，請儲存該憑證。

5. 回到路由器畫面，進入**本機憑證**，按下**匯入**按鈕並瀏覽檔案以匯入憑證至路由器中。當您完成這個動作時，請按頁面更新，您就可以看見如下的視窗。

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

| Name | Subject | Status | Modify |
|---|---|---|---|
| Local | /C=TW/ST=HC/L=HC/O=Draytek/O... | Requesting | View Delete |

GENERATE IMPORT REFRESH

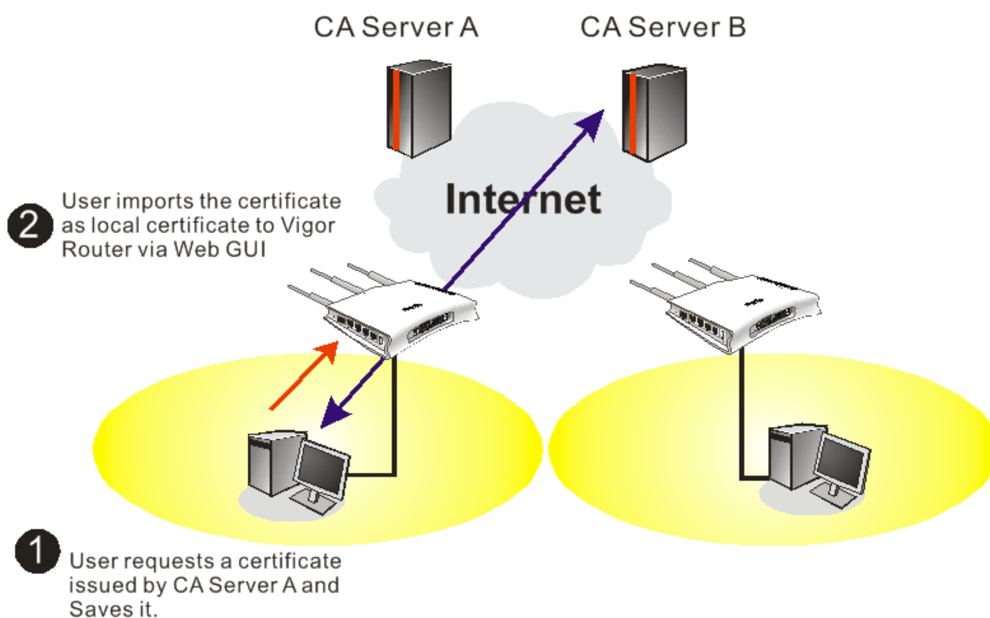
X509 Local Certificate


-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH
EwJIQzEQMA4GA1UEChMHRHJheXRlazELMAkGA1UECxMCUkQxIjAgBgkqhkiG9w0B
CQEWE3N1cHBvcnRAZHJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTU5HQvXpAzcrgJBGrikTUBX
a1X//fgnEccQA2LPSQIQ85Qychwq07Bm0EDf10wHwCalAZQoGvIiODMC7f5w9xA8
m6+0f4xZ4QQnjXXgciC0Bj1iAa6MLScelsynZhkgnQ1QN5uFAgMBAAGgADANBgkq
hkiG9w0BAQUFAAOBgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYDZefCmGfX
9yojHpstNsmWsMRuAwGeKCWc8S/gLtHhr6iccMoToQFx/LWdaEPU5LqryBKKgC9t
eorpDa1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvclhWFSXKVLU7g==
-----END CERTIFICATE REQUEST-----

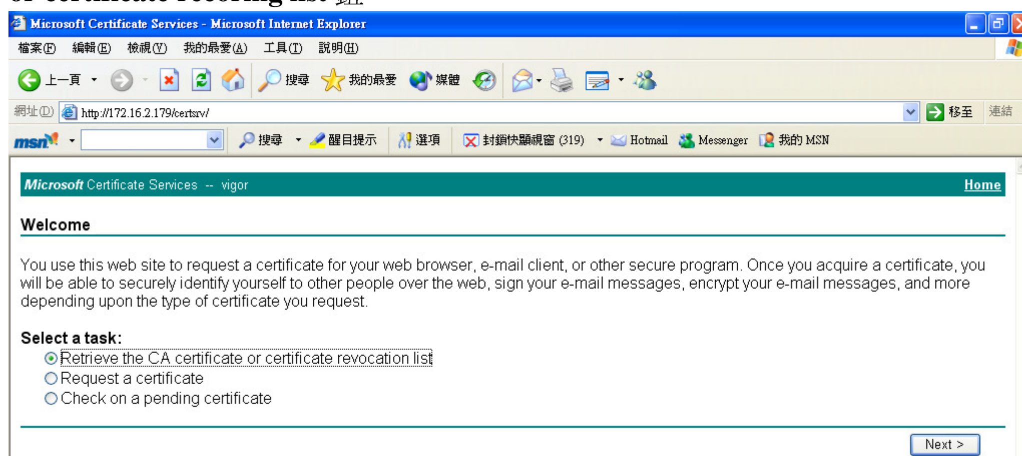

6. 您也可以重新檢視憑證的細節資訊，請按**檢視**按鈕。

| | |
|---|---|
| Name : | Local |
| Issuer : | /C=US/CN=vigor |
| Subject : | /emailAddress=press@draytek.com/C=TW/O=Draytek |
| Subject Alternative Name : | DNS:draytek.com |
| Valid From : | Aug 30 23:08:43 2005 GMT |
| Valid To : | Aug 30 23:17:47 2007 GMT |

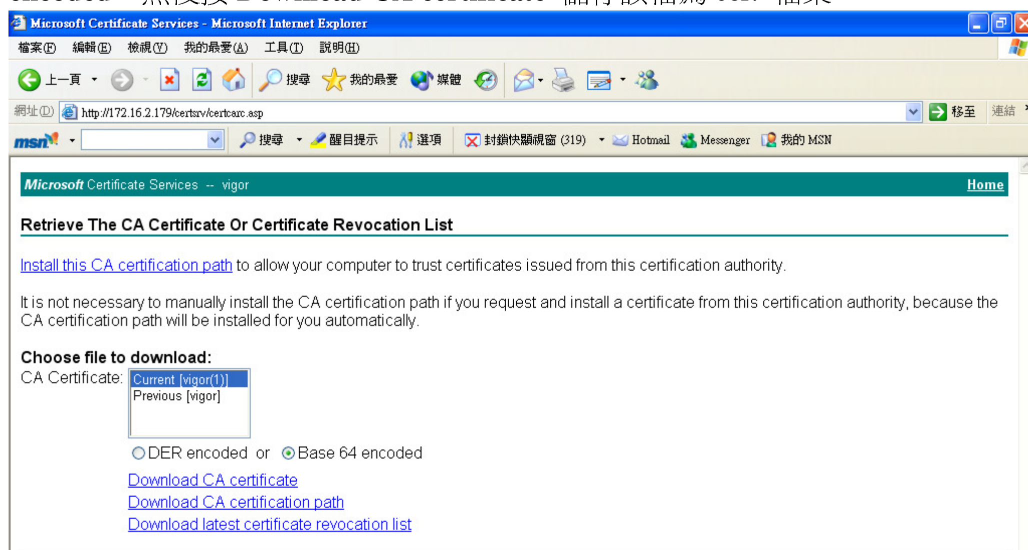
## 5.8 提出 CA 憑證要求並將之設定為 Windows CA 伺服器上具公信力之憑證




1. 使用瀏覽器連接至 CA 伺服器以取得您想要的憑證。按下 **Retrive the CA certificate or certificate recoring list** 鈕。



2. 在 **Choose file to download** 區中，按 CA Certificate **Current** 以及 **Base 64 encoded**，然後按 **Download CA certificate** 儲存該檔爲 cer. 檔案。




3. 回到路由器網頁設定畫面，進入**具公信力之 CA 憑證**，按**匯入**按鈕並瀏覽檔案以匯入憑證。當您完成這個動作之後，請按更新頁面察看最新的憑證使用狀況。

**Certificate Management >> Trusted CA Certificate**

**X509 Trusted CA Certificate Configuration**

| Name | Subject | Status | Modify |
|---|---|---|---|
| Trusted CA-1 | /C=US/CN=vigor | Not Yet Valid | View Delete |
| Trusted CA-2 | --- | --- | View Delete |
| Trusted CA-3 | --- | --- | View Delete |

IMPORT REFRESH

4. 您也可以重新檢視憑證的細節資訊，請按**檢視**按鈕。

| | |
|---|---|
| Name : | Trusted CA-1 |
| Issuer : | /C=US/CN=vigor |
| Subject : | /C=US/CN=vigor |
| Subject Alternative Name : | DNS:draytek.com |
| Valid From : | Aug 30 23:08:43 2005 GMT |
| Valid To : | Aug 30 23:17:47 2007 GMT |

Close

**注意:**在設定憑證之前，請先至**系統維護>>日期與時間**頁面中重新設定路由器的時間。

# 6 疑難排解

這個章節將幫助您解決安裝完成路由器後，卻無法順利登入網際網路的情形。請依照以下的步驟檢查您路由器的基本設定。

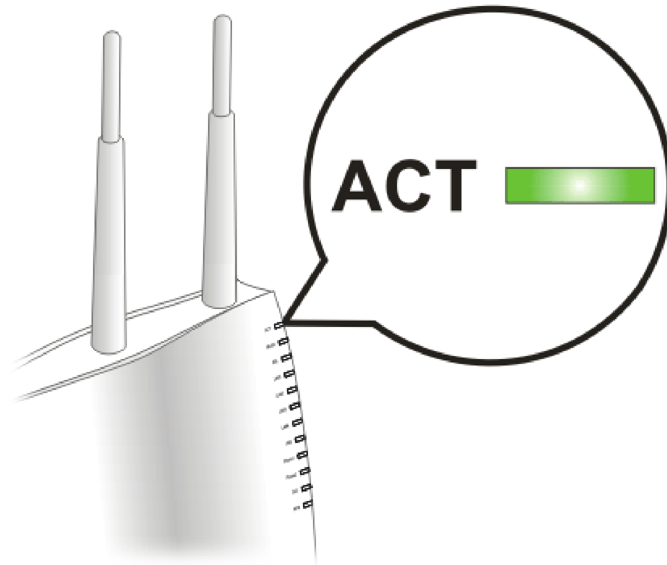
- 檢查硬體狀態是否正常。
- 檢查您個人電腦內的網路連線設定是否正確。
- 從您的個人電腦 Ping 路由器是否正確。
- 檢查你的 ISP 設定是否正確。
- 必要時，請還原路由器出廠預設值。

如果路由器的設完全正確但路由器仍舊無法正常運作，建議與購買的經銷商聯絡以協助您進行設定。

## 6.1 檢查硬體狀態是否正常

依照以下的步驟去確認路由器的硬體狀態。

1. 檢查電源線、區域網路(LAN)/無線區域網路(WLAN)電纜是否連線。詳細安裝資料，請參照 **1.3 硬體安裝**。
2. 開啓路由器後，確認 ACT 燈號是否爲每秒閃動一次，並確認相對應的 LAN 燈號是否亮起。




3. 如果不是，表示硬體狀態在某些設定下發生錯誤，請回到 **1.3 硬體安裝**重新設定並再嘗試確認安裝無誤。

## 6.2 檢查您個人電腦內的網路連線設定是否正確

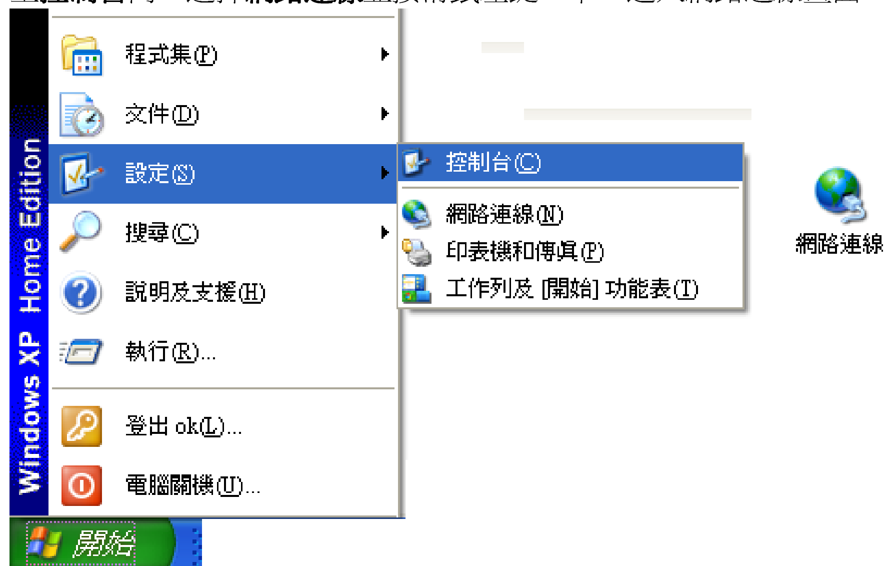
有時連線失敗是在於網路連線設定錯誤。若在嘗試上述的步驟之後，網路連結依然失敗，請依照以下的步驟確定網路連線設定是否正常。

### 適用於 Windows

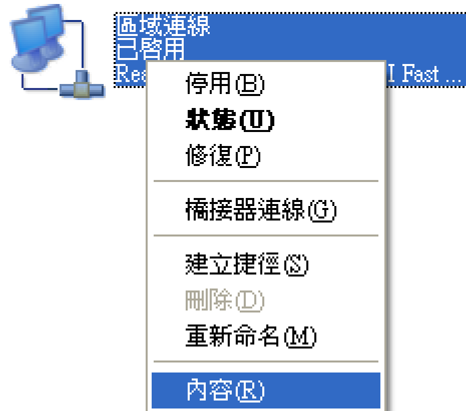


下列的範例是以 Windows XP 作業系統為基礎。若您的電腦採用其他的作業系統，請參照相似的步驟或至 www.draytek.com 查閱相關的技術文件說明。

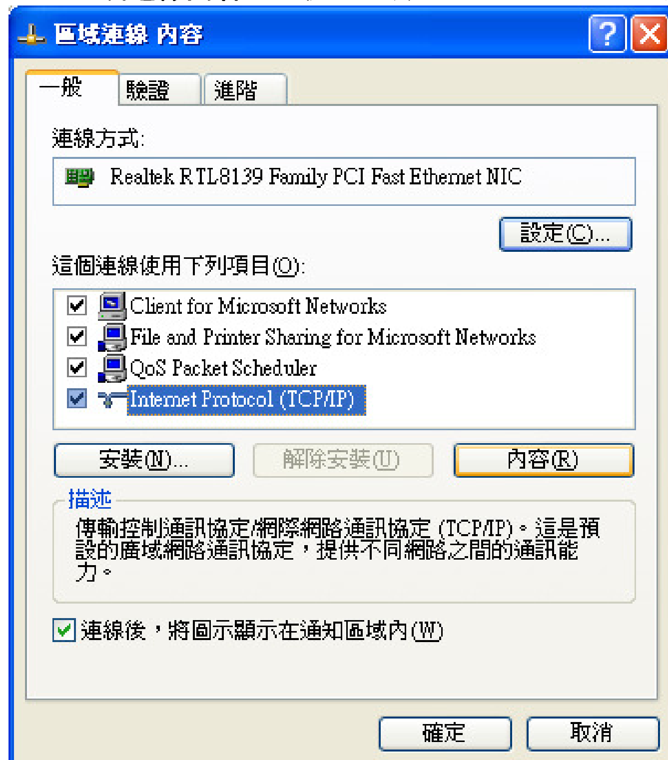
1. 至**控制台**內，選擇**網路連線**並按滑鼠左鍵二下，進入網路連線畫面。



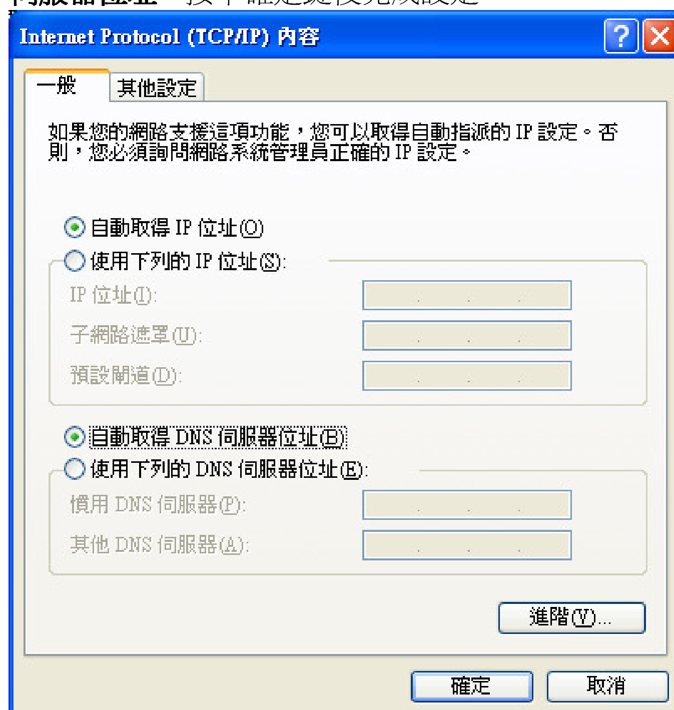

2. 選擇**區域連線**按滑鼠右鍵，選擇**內容**。



3. 進入**區域連線內容**畫面後，選擇 **Internet Protocol (TCP/IP)**，按下**內容**鍵。

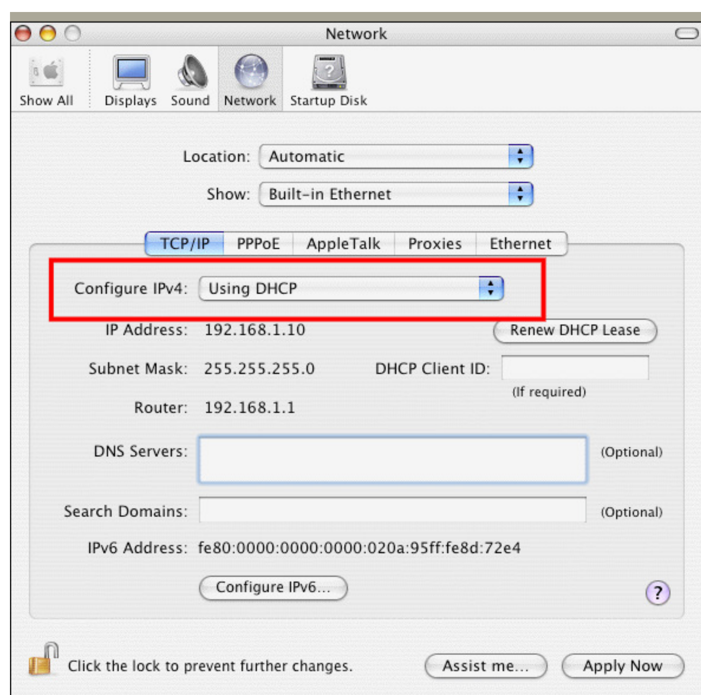



4. 進入 **Internet Protocol (TCP/IP)內容**畫面後，選擇**自動取得 IP 位址**及**自動取得 DNS 伺服器位址**，按下確定鍵後完成設定。




## 適用於 MacOS

1. 在桌面上選擇目前所使用的 MacOS 磁碟機按滑鼠 2 下。
2. 選擇 **Applications** 檔案夾中的 Network 檔案夾。
3. 進入 **Network** 畫面，在 Configure IPv4 選項中，選擇 **Using DHCP**。


Network
Show All
Displays
Sound
Network
Startup Disk
Location: Automatic
Show: Built-in Ethernet
TCP/IP
PPPoE
AppleTalk
Proxies
Ethernet
Configure IPv4: Using DHCP
IP Address: 192.168.1.10
Renew DHCP Lease
Subnet Mask: 255.255.255.0
DHCP Client ID:
(If required)
Router: 192.168.1.1
DNS Servers:
(Optional)
Search Domains:
(Optional)
IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4
Configure IPv6...
Click the lock to prevent further changes.
Assist me...
Apply Now

## 6.3 從您的個人電腦 Ping 路由器是否正確

路由器的預設閘道爲 192.168.1.1. 因爲某些理由，你可能需要使用 " ping " 指令檢查路由器的連結狀態。重要在於電腦是否收到來自 192.168.1.1 的回應，如果沒有，請檢查個人電腦上的 IP 位址。我們建議您將網際網路連線設定爲自動取得 IP 位址。(請參照 6.2 檢查您個人電腦內的網路連線設定是否正確)，請依照以下的步驟正確地 ping 路由器。

### 適用於 Windows

1. 開啓**命令提示字元視窗**（ 開始功能表選單 → 執行 ）。
2. 輸入 **command** (適用於 Windows 95/98/ME )或 **cmd** (適用於 Windows NT/ 2000/XP)。DOS 命令提示字元視窗將會出現。

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. 輸入 **ping 192.168.1.1** 並按下 **Enter**，如果連結成功，電腦會收到來自 192.168.1.1 的回應 "**Reply from 192.168.1.1: bytes=32 time<1ms TTL=255**"。
4. 如果連結失敗，請確認個人電腦的 IP 位址設定是否有誤。

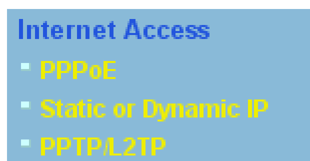
### 適用於 MacOs (終端機)

1. 在桌面上選擇目前所使用的 Mac OS 磁碟機按滑鼠二下。
2. 選擇 **Applications** 檔案夾中的 **Utilities** 檔案夾。.
3. 滑鼠按二下 **Terminal**；終端機的視窗將會跳出顯現在螢幕。
4. 輸入 **ping 192.168.1.1** 並且按下 **Enter** 鍵。如果連結正常，終端機視窗會出現"**64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" 的訊息。

```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

## 6.4 檢查您的 ISP 設定是否正確

從 Web 設定介面上，點選**網際網路連線設定**，檢查 ISP 設定。




### 針對 PPPoE 使用者

1. 檢查是否已選取**啓用**模式。
2. 檢查輸入的**使用者名稱**及**密碼**是否與 ISP 給您的資料相符。

Internet Access >> PPPoE

PPPoE Client Mode

| PPPoE Setup | | PPP/MP Setup | |
|---|---|---|---|
| PPPoE Link | ⦿ Enable ○ Disable | PPP Authentication | PAP or CHAP |
| ISP Access Setup | | ☑ Always On | |
| Username | 123 | Idle Timeout | -1 second(s) |
| Password | ●●● | IP Address Assignment Method (IPCP) | WAN IP Alias |
| Index(1-15) in Schedule Setup: | | Fixed IP | ○ Yes ⦿ No (Dynamic IP) |
| => | , , , | Fixed IP Address | |
| WAN Connection Detection | | ⦿ Default MAC Address | |
| Mode | ARP Detect | ○ Specify a MAC Address | |
| Ping IP | | MAC Address: | 00 .50 .7F :9A .32 .71 |
| TTL: | | | |

OK

### 針對固定/動態 IP 使用者

1. 檢查是否已選取**啓用**模式。

2. 檢查輸入的 **IP 位址，子網路遮罩**及**閘道 IP 位址**是否與 ISP 給您的資料相符。

Internet Access >> Static or Dynamic IP

Static or Dynamic IP (DHCP Client)

| Access Control | WAN IP Network Settings [WAN IP Alias] |
|---|---|
| Broadband Access ⦿ Enable ○ Disable | ○ Obtain an IP address automatically |
| Keep WAN Connection | Router Name * |
| ☐ Enable PING to keep alive | Domain Name * |
| PING to the IP 0.0.0.0 | * : Required for some ISPs |
| PING Interval 0 minute(s) | ⦿ Specify an IP address |
| WAN physical type | IP Address 192.168.5.26 |
| Auto negotiation | Subnet Mask 255.255.255.0 |
| WAN Connection Detection | Gateway IP Address 192.168.5.1 |
| Mode ARP Detect | ⦿ Default MAC Address |
| Ping IP | ○ Specify a MAC Address |
| TTL: | MAC Address: 00 .50 .7F :9A .32 .71 |
| RIP Protocol | DNS Server IP Address |
| ☐ Enable RIP | Primary IP Address |
| | Secondary IP Address |

OK

## 針對 PPTP 使用者

1. 檢查是否已選取**啓用**模式。

Internet Access >> PPTP

PPTP Client Mode

| PPTP Setup | PPP Setup |
|---|---|
| PPTP Link ⦿ Enable ○ Disable | PPP Authentication PAP or CHAP |
| PPTP Server 10.0.0.138 | ☑ Always On |
| ISP Access Setup | Idle Timeout -1 second(s) |
| Username 123 | IP Address Assignment Method (IPCP) |
| Password ●●● | Fixed IP ○ Yes ⦿ No (Dynamic IP) |
| Index(1-15) in Schedule Setup: | Fixed IP Address |
| => , , , | WAN IP Network Settings |
| | ○ Obtain an IP address automatically |
| | ⦿ Specify an IP address |
| | IP Address 10.0.0.150 |
| | Subnet Mask 255.0.0.0 |

OK

2. 檢查輸入的**使用者名稱**及**密碼**是否與 ISP 給您的資料相符。
3. 檢查輸入的 **IP 位址**及**子網路遮罩**是否與 ISP 給您的資料相符。

## 6.5 還原路由器原廠預設組態

有時，錯誤的連線設定可以藉由還原廠預設組態來重新設定，您可以利用軟體重置或硬體重置的方法還原路由器設定值。



**警告**：在使用原廠預設組態後，您之前針對分享器所調整的設定都將恢復成預設值。請確實記錄之前路由器所有的設定，預設出廠的密碼為空白。

### 軟體重置

您可以利用 Web 介面將路由器的重置成原廠預設組態。

點選網頁左下方**系統維護**的**重啓路由器**選項。選擇**使用原廠預設組態**，等待 3 秒以後，路由器將重新啓動並將所有設定還原成原廠預設組態。

System Maintenance >> Reboot System

Reboot System

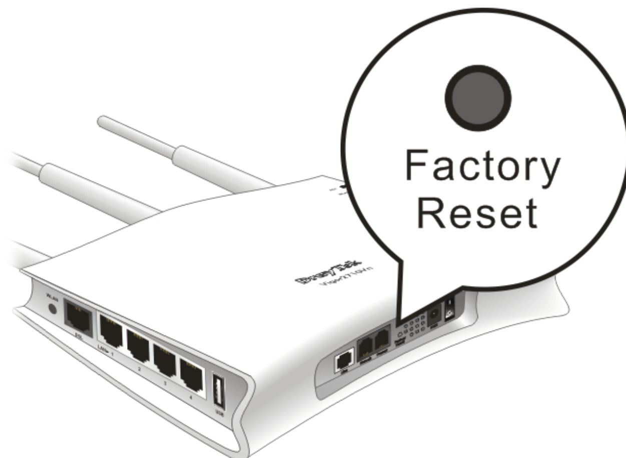
Do you want to reboot your router ?

- Using current configuration
- Using factory default configuration

OK

### 硬體重置

當路由器正在運作時（ACT 燈號閃爍），壓住 **Factory Reset** 鈕超過 5 秒，當您看到 ACT 燈號開始快迅閃爍時，請鬆開 **Factory Reset** 鈕，此時，路由器將會還原成原廠預設組態。




在恢復原廠預設組態後，您可以再次依照您所需設定路由器。

## 6.6 連絡您的經銷商

假如經過多次嘗試設定後，路由器仍舊無法正常運作，請立即與經銷商聯絡